



## Calhoun: The NPS Institutional Archive DSpace Repository

---

Theses and Dissertations

1. Thesis and Dissertation Collection, all items

---

2006-03

### Implementing maritime domain awareness

Watts, Robert B.

Monterey, California. Naval Postgraduate School

---

<http://hdl.handle.net/10945/2945>

*Downloaded from NPS Archive: Calhoun*



Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

Dudley Knox Library / Naval Postgraduate School  
411 Dyer Road / 1 University Circle  
Monterey, California USA 93943

<http://www.nps.edu/library>



**NAVAL  
POSTGRADUATE  
SCHOOL**

**MONTEREY, CALIFORNIA**

**THESIS**

**IMPLEMENTING MARITIME DOMAIN AWARENESS**

by

R. B. Watts

March 2006

Thesis Advisor:  
Second Reader:

Jeffrey Kline  
C. Martoglio

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

**REPORT DOCUMENTATION PAGE**

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

|  |   |  |   |
|--|---|--|---|
| <b>1. AGENCY USE ONLY (Leave blank)</b>  | <b>2. REPORT DATE</b><br>March 2006                             | <b>3. REPORT TYPE AND DATES COVERED</b><br>Master's Thesis     |   |
| <b>4. TITLE AND SUBTITLE:</b> Implementing Maritime Domain Awareness   |   | <b>5. FUNDING NUMBERS</b>                                      |   |
| <b>6. AUTHOR(S)</b> Watts, Robert B.   |   |  |   |
| <b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b><br>Naval Postgraduate School<br>Monterey, CA 93943-5000  |   | <b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>                |   |
| <b>9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b><br>N/A   |   | <b>10. SPONSORING/MONITORING AGENCY REPORT NUMBER</b>          |   |
| <b>11. SUPPLEMENTARY NOTES</b> The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.  |   |  |   |
| <b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b><br>Approved for public release; distribution is unlimited  |   | <b>12b. DISTRIBUTION CODE</b>                                  |   |
| <b>13. ABSTRACT (maximum 200 words)</b><br>As an attempt to gain understanding of everything in the global maritime environment that can impact the security of the United States, the Maritime Domain Awareness initiative is one of the most ambitious projects ever undertaken by the U.S. government. Information that falls under the prevue of MDA is tremendously diverse and complex, having application in the regulatory, law enforcement, and military arenas. As such, MDA is a multi-agency effort that encompasses 16 respective departments, agencies, and organizations working toward one common goal of shared information. Given that each of these organizations operates under policies and procedures that are radically different, effective MDA requires the design of a construct that fuses multi-agency information in such a way that it can be effectively shared among all agencies. This thesis argues that current infrastructure in the Coast Guard and Navy can be used to obtain MDA through a formal linking process that fuses multi-agency information on the tactical, regional, and strategic levels for sharing and dissemination to appropriate forces for action. |   |  |   |
| <b>14. SUBJECT TERMS</b> Maritime Domain Awareness, Homeland Security, Homeland Defense, JHOC, MFIC, NMIC  |   | <b>15. NUMBER OF PAGES</b><br>81                               |   |
| <b>16. PRICE CODE</b>  |   |  |   |
| <b>17. SECURITY CLASSIFICATION OF REPORT</b><br>Unclassified   | <b>18. SECURITY CLASSIFICATION OF THIS PAGE</b><br>Unclassified | <b>19. SECURITY CLASSIFICATION OF ABSTRACT</b><br>Unclassified | <b>20. LIMITATION OF ABSTRACT</b><br>UL |

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)  
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

**IMPLEMENTING MARITIME DOMAIN AWARENESS**

Robert B. Watts  
Commander, United States Coast Guard  
M.A., Old Dominion University, 1993

Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES  
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL  
March 2006**

Author: Robert B. Watts

Approved by: Jeffrey Kline  
Thesis Advisor

Charles Martoglio  
Second Reader

Douglas Porch  
Chairman, National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

As an attempt to gain understanding of everything in the global maritime environment that can impact the security of the United States, the Maritime Domain Awareness initiative is one of the most ambitious projects ever undertaken by the U.S. government. Information that falls under the purview of MDA is tremendously diverse and complex, having application in the regulatory, law enforcement, and military arenas. As such, MDA is a multi-agency effort that encompasses 16 respective departments, agencies, and organizations working toward one common goal of shared information. Given that each of these organizations operates under policies and procedures that are radically different, effective MDA requires the design of a construct that fuses multi-agency information in such a way that it can be effectively shared among all agencies. This thesis argues that current infrastructure in the Coast Guard and Navy can be used to obtain MDA through a formal linking process that fuses multi-agency information on the tactical, regional, and strategic levels for sharing and dissemination to appropriate forces for action.

**THIS PAGE INTENTIONALLY LEFT BLANK**

## TABLE OF CONTENTS

|   |   |    |
|---|---|----|
| I.  | INTRODUCTION.....                                   | 1  |
| A.  | OBJECTIVE .....                                     | 3  |
| B.  | METHODOLOGY .....                                   | 4  |
| C.  | TERMS OF REFERENCE .....                            | 4  |
| D.  | NOTES ON SOURCES .....                              | 6  |
| E.  | EXPECTED RESULTS OF THIS THESIS .....               | 6  |
| II.   | CURRENT STRATEGIC GUIDANCE AND INFRASTRUCTURE ..... | 7  |
| A.  | WHY MDA? .....                                      | 7  |
| B.  | WHAT IS MDA?.....                                   | 9  |
| C.  | MDA: THE MECHANICS .....                            | 12 |
| III.  | MDA ORGANIZATIONAL CONSTRUCT .....                  | 17 |
| A.  | TACTICAL MDA .....                                  | 18 |
| B.  | REGIONAL/OPERATIONAL MDA .....                      | 25 |
| C.  | STRATEGIC MDA .....                                 | 31 |
| D.  | SUMMARY OF THE CURRENT INFRASTRUCTURE MODEL .....   | 39 |
| IV.   | ALTERNATIVE MDA MODELS .....                        | 41 |
| A.  | MARITIME NORAD .....                                | 42 |
| B.  | JIATF .....   | 45 |
| V.  | SUMMARY .....                                       | 51 |
| APPENDIX 1: HOMELAND SECURITY AND HOMELAND DEFENSE..... |   | 53 |
| A.  | BACKGROUND: WHY TWO MISSIONS?.....                  | 53 |
| APPENDIX 2: MDA LEGAL BRIEF .....                       |   | 57 |
| LIST OF REFERENCES .....                                |   | 61 |
| INITIAL DISTRIBUTION LIST .....                         |   | 67 |

THIS PAGE INTENTIONALLY LEFT BLANK

## **LIST OF FIGURES**

|           |                                       |    |
|-----------|---------------------------------------|----|
| Figure 1. | MDA Tracking Process.....             | 14 |
| Figure 2. | MDIZ .....                            | 15 |
| Figure 3. | Sector Command Center Structure ..... | 22 |
| Figure 4. | JHOC/COP.....                         | 24 |
| Figure 5. | MFIC.....                             | 30 |
| Figure 6. | Current Infrastructure Model .....    | 37 |

THIS PAGE INTENTIONALLY LEFT BLANK

## **ACKNOWLEDGMENTS**

MDA is an evolving concept. Many of the people directly involved with the continued planning and implementation of MDA were critical in the writing of this thesis, providing a unique “hands on” perspective in their particular area of expertise. My thesis advisors, Captain Jeffrey Kline, USN (ret) and RDML Charles Martoglio, USN, provided not only continuous advice but also keen strategic insight regarding the role MDA played in Maritime Domain Protection and the National Maritime Strategy. Mr. Jeff High, who one day will be remembered as the “father” of MDA and his able successor, RDML Joe Nimmich, USCG, granted in-depth and candid interviews on the history of MDA and its future implications for the Coast Guard and Navy. Ms Wendy Kay provided a detailed unclassified view of naval strategic intelligence, while CDR Randy Dykes, USN and Mr. Guy Thomas, as long-time MDA planners, were invaluable for their review of this thesis and their insight. Finally, special thanks to Dr Lauren Wollman for her inexhaustible academic acumen in preparing this document.

THIS PAGE INTENTIONALLY LEFT BLANK

## I. INTRODUCTION

The Maritime Domain Awareness (MDA) initiative is one of the largest strategic security measures enacted by the U.S. government since the 9/11 attacks.<sup>1</sup> Although the attacks on 9/11 came from the air, the fact is undeniable that the United States is economically (and militarily) dependent upon the sea for livelihood and to project national power.<sup>2</sup> There is little argument that our maritime infrastructure is vulnerable, and that a potential enemy can use the sea to gain access to our nation. The key to defeating this potential threat is knowledge, specifically information that focuses on who (or what) is operating in the maritime domain. MDA is an attempt to gain global knowledge of all actions occurring in the maritime domain that can affect the security of the United States. This effort has grown from a Coast Guard/Navy initiative to involve 16 respective government Agencies and Departments. Although these groups agree that some form of MDA is needed (and, in fact, its implementation has been mandated by Presidential direction),<sup>3</sup> the actual implementation of MDA is problematic. Designed as an information initiative, how MDA is to be implemented across such a broad agency spectrum to unify the diverse capabilities of each remains unclear. Should MDA rely on the infrastructure agencies currently have in place, or the responsibility of an entirely new command dedicated to its implementation? This answer is both illusive and, given the number of agencies involved and the wide range of MDA objectives, controversial.

This thesis argues that use of current infrastructure is the most efficient means to obtain MDA, aligning and merging military and civilian capabilities in a logical maritime construct toward a common objective. Fundamental to the success of this model will be

---

<sup>1</sup> The original Maritime Domain Awareness initiative pre-dates 9/11. Designed as an expansion of the Coast Guard's Special Interest Vessel (SIV) tracking program under Admiral Loy, the initial study examined means by which specific vessels could be effectively tracked in the broad approaches to the United States. The attacks on 9/11 moved this program to the immediate forefront of Service priorities for the Coast Guard and radically altered the size, scope, and objectives of the program. Jeffrey High, interview by Robert Watts, notation, 25 March 2005, Coast Guard Headquarters, Washington D.C.

<sup>2</sup> *National Plan to Achieve Maritime Domain Awareness* (Washington D.C.: U.S. Coast Guard, Pre-Decisional Working Draft, 28 April 05), 3.

<sup>3</sup> *National Security Presidential Directive NSPD-41/Homeland Security Presidential Directive HSPD-13* (Washington D.C. The White House, December 2004), 3.

an inter-agency establishment of liaison positions and development of joint fusion centers that can act as collection and dissemination points for the vast degree of information required for effective MDA. This will require the drafting of inter-agency agreements, the design of a common communication and operational picture, and establishment of a common multi-agency information system (COP) on the strategic, regional, and tactical levels of MDA.

Current infrastructure offers a number of advantages to rapid and effective MDA implementation. Although MDA is relatively new, the fundamental concept is not; both Navy and Coast Guard, along with a host of maritime intelligence agencies, have been practicing some form of ship tracking as part of their operations for years. Prior to 9/11 these efforts had a tendency to be focused primarily on specific agency objectives. Coast Guard intelligence, for example, emphasized various types of law enforcement activity, while the Navy examined areas of potential military threat. It is important to note that while these efforts were agency specific, the facilities and expertise developed during this time period share many common protocols that ease merging into one multi-agency MDA construct.

A survey of current maritime intelligence infrastructure demonstrates that many of these facilities were rapidly modified to meet the new threat in the immediate aftermath of 9/11. On the tactical level, Coast Guard created a number of new harbor operations centers designed to re-direct traditional law enforcement missions toward a potential terrorist threat. This initiative subsequently expanded to include Navy and other multi-agency partners working in individual ports, resulting in the creation of a number of experimental Joint Harbor Operations Centers (JHOCs) that are ideal for the tactical implementation of MDA. On the regional/operational level, most DHS and DoD agencies created some form of “fusion” center for anti-terrorist intelligence. The Coast Guard’s Maritime Intelligence Fusion Centers (MIFCs) established links with many of the agencies currently involved in the MDA effort, creating an effective merger of military and law enforcement information by both DHS and DoD. Strategically, the Navy’s National Maritime Intelligence Center (NMIC) capitalized on existing protocol

with the Coast Guard to provide analysis on worldwide shipping trends and activity that had new potential terrorist implications for national security.

While it is true these efforts in the intelligence and operational communities can potentially support MDA, recognizing that this infrastructure exists is not enough. In order for MDA to become a reality, these groups must be linked under one common operating protocol to aide in the flow of information between strategic, regional, and tactical levels. This can be accomplished through identifying the best infrastructure on each level, then establishing inter-agency cooperation through the use of liaison positions and devising common operating procedures. Critical to this effort will be the design of a common operating picture that can electronically link MDA facilities for rapid and effective information exchange between the tactical, regional, and strategic levels of fusion.

#### **A. OBJECTIVE**

This thesis' objective is to provide a logical construct for the use of current infrastructure to obtain MDA. Current infrastructure is by no means the only proposal being considered by national planners. In the immediate aftermath of 9/11 the term "Maritime NORAD" became very popular, evoking images of a coastline controlled by various sensors linked to a new command that operated along the same lines as U.S-Canadian air defense. The Maritime NORAD solution proposes the creation of such a command for MDA, with associated response forces to deal with homeland security/homeland defense (HLS/HLD) incidents. Using a Joint Inter-Agency Task Force (JIATF) command, a very popular military solution for dealing with specific mission areas, has also been proposed as a solution for achieving MDA. But MDA's multi-agency and informational (vice operational) nature makes these solutions inappropriate. Although mission focused, another command dedicated to HLS/HLD blurs responsibilities between DHS and DoD and requires a complete redesign of the current homeland defense infrastructure. This alternate is neither cost effective nor, given the number of commands already in place to perform this mission, practical.

As a key component of the National Maritime Strategy, MDA is a vital link to homeland security that must be implemented expeditiously and effectively. Although several options exist for its implementation, effective MDA is best accomplished through the identification of current infrastructure within DHS and DoD that has experience in the maritime domain, then capitalizing on this expertise by designing a fusion construct that merges tactical, regional, and strategic structures towards a common goal.

## **B. METHODOLOGY**

This paper will examine recent innovations by the Coast Guard and Navy following the 9/11 attacks and how these innovations can be linked in an MDA construct that best leverages the various capabilities of participating agencies vis a vis current strategic guidance. It presents a logical tactical, operational, and strategic construct that capitalizes on existing agency strengths linked toward achieving a common objective. Although many of the organizations and commands described in this thesis exist today, examining how these entities can interact to implement MDA will be largely theoretical as, to date, the final form of MDA remains in debate. The use of current infrastructure will be compared with other proposed MDA alternatives, specifically the creation of a Maritime NORAD or the formation of a Joint Inter-Agency Task Force (JIATF) specifically designed for MDA.

## **C. TERMS OF REFERENCE**

MDA is a joint interagency effort. Originally proposed by the Coast Guard, MDA has since expanded to become an equal effort between the Department of Homeland Security (DHS) and Department of Defense (DOD).<sup>4</sup> DHS and DOD are, in turn, responsible for Homeland Security (HLS) and Homeland Defense (HLD)

---

<sup>4</sup> The Coast Guard remains the “Lead Federal Agency” (LFA) for MDA. See *Maritime Strategy for Homeland Security* (Washington D.C: U.S. Coast Guard, July 2002), 1.

respectively.<sup>5</sup> In the context of HLS/HLD operations it is important to note in this case what MDA is *not*. MDA is not the effort to exercise command and control over forces conducting operational missions. Rather, MDA is the obtaining and dissemination of *information* relative to these mission areas that can subsequently be used by DHS and DOD operational forces. MDA is a force multiplier, bringing together a vast array of information that can be disseminated for appropriate action. MDA provides members of the maritime protection community with information, intelligence, and products to support their homeland security strategies and subsequent operational decisions.<sup>6</sup>

In the classical military definition, it would seem that MDA is nothing more than intelligence. This is true in the sense that intelligence—both military and law enforcement—is crucial to the execution of MDA. MDA, however, goes beyond traditional intelligence as it considers a far greater pool of information that would not normally be considered “intelligence.” Friendly information, port activity, recreational boating, merchant activity, crew lists, manifests, and other peripheral activities in the maritime domain are merged with threat information into one comprehensive “picture.” This “Common Operating Picture” (COP) can then be used as an enabler for command and control. MDA is very much a “two way street” between the provider of MDA—defined as some form of fusion and analysis center—and operational units in the field. Unlike traditional intelligence which has a tendency to obtain specific (and often stove piped) information specific about a singular threat, MDA seeks to fuse data across interagency lines in a highly cyclical relationship between operational forces on the

---

<sup>5</sup> Homeland Security (HLS) is defined as “a concentrated national effort to prevent terrorist attacks within the United States, reduce America’s vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.” Homeland Defense (HLD) is defined as “the protection of U.S. sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression.” See *Strategy for Homeland Defense and Civil Support* (Washington D.C: Department of Defense, Final Coordination Draft, Jan 2005), 10. While it is not the purpose of this thesis to focus on the differences between these missions, it would be fair to say that the vast bulk of maritime security actions—vessel tracking, boarding, and search—will be considered HLS. HLD actions are generally confined to a very specific, known threat where immediate military (destructive) action is required and are therefore far rarer events than day-to-day HLD operations. MDA is an enabler for both HLS and HLD. See *The National Strategy for Homeland Security* (Washington D.C: Office of Homeland Security, 2002), 2, and *Strategy for Homeland Defense*, 10.

<sup>6</sup> *Concept of Operations (CONOPS): Maritime Domain Awareness*, Draft 1.29 (Washington D.C: U.S. Coast Guard, November 2004), 2.

tactical and strategic levels which both feed the COP and take information from it. This element will be examined in detail in following chapters.

#### **D. NOTES ON SOURCES**

The MDA concept is continuously evolving, and in response various agencies have generated a number of draft plans, documents and briefings in creating a final MDA implementation plan for Presidential signature. As a Navy Staff planner, the author has reviewed most of these plans for official comment by DOD, as well as attended numerous senior briefings in the planning process. Many concepts cited in early planning documents were cut from the final plan, not because they were invalid or non-contributory to MDA, but rather due to the broader scope desired for a final Presidential review.<sup>7</sup> Since these concepts are valid and will be revisited when the plan's details are worked out, this paper cites various drafts and coordination versions of the original MDA plan. All of the briefings cited in this thesis were attended by the author. When specific briefing personnel are cited, direct questions related to this thesis were asked and the briefers advised that their answers would become part of this research. At no time was any classified or sensitive information used in writing this thesis.

#### **E. EXPECTED RESULTS OF THIS THESIS**

At this writing MDA is in a critically formulative phase. By Presidential Directive some form of MDA strategy exists after 1 July 2005. The exact form this MDA system will take and its actual construct has commended and is being developed by an officially sanctioned Implementation Team. It is their work this thesis addresses. It will provide a recommended organizational construct that can be used to successfully implement the MDA strategy in a rapid and effective manner, and is intended for presentation to the MDA directorate for use in developing the implementation portion of the MDA plan.

---

<sup>7</sup> For example, the concept of the Maritime Detection and Interdiction Zone (MDIZ) is central to MDA as a layered defense/guide for detection and tracking metrics. This concept is very much alive in MDA operational planning and was cited in the early versions of the National Plan, but was cut from the final version as far too tactical for a national level document.

## II. CURRENT STRATEGIC GUIDANCE AND INFRASTRUCTURE

### A. WHY MDA?

Throughout its history the United States has been a global maritime nation, dependent upon the oceans for economy, welfare, and defense. In the modern era emphasis on globalization and the world economy has increased this dependence considerably. The numbers representing the sea's geographic expanse and our reliance upon it are illustrative of the vast problem of maritime awareness. There are some 95,000 miles of United States' coastline and 3.4 million square miles of territorial seas and exclusive economic zones in the U.S. maritime domain.<sup>8</sup> Connecting the continental United States to this zone are over 1000 harbors and ports, 361 of which are cargo capable. Through these ports enter approximately 21,000 containers daily, representing 95 percent of the nation's overseas cargo, and including 100 percent of our petroleum imports.<sup>9</sup> In addition to pure commerce, there are 76 million recreational boaters in the United States. Six million cruise ship passengers visit U.S. ports annually.<sup>10</sup> In the strategic/military sense, a substantial portion of U.S. national power relies on the sea, both in the form of traditional Navy Carrier Strike groups that deploy from ports in the continental United States and the subsequent ability to reinforce deployed forces overseas. Without unimpeded access to the sea, the ability for the United States to project national power is limited to what can be airlifted.

The potential threats associated with the maritime, and especially the coastal, environment have always been wide-ranging and diverse, relying on a combination of asymmetric offensive tactics while exploiting the variety of the littoral. This vulnerability has been recognized and exploited by enemies in the past. During the First

---

<sup>8</sup> *The National Strategy for Maritime Security* (Washington D.C: NSMS Writing Team, Working Draft Paper, Feb 2005), 4.

<sup>9</sup> J.Z. Hecker, "Port Security: Nation Faces Formidable Challenges in Making New Initiative Successful," *GAO Publication No. GAO-2-993T* (Washington D.C.: United States General Accounting Office, August 2002), 3.

<sup>10</sup> *National Strategy for Maritime Security*, 11.

and the Second World War, the coastline of the Untied States was subject to attack from enemy submarines, mines, and special operations teams. The Nazi U-boat offensive during the Second World War was particularly effective, destroying over 400 ships in an almost completely undefended littoral.<sup>11</sup> Defeat of this threat, which caused considerable damage to the U.S. war effort, required the aggressive use of intelligence, a dedicated surveillance effort, and a coordinated, multi-agency effort to defeat the enemy with non-traditional methods.<sup>12</sup> During the Cold War it was assumed this scenario would repeat itself using modern technology, and the coastline of the United States would be subject to attack by conventional and unconventional forces of the Soviet Navy targeting infrastructure vital to overseas reinforcement and re-supply. Accordingly, an entirely new Coast Guard-Navy command structure—the Maritime Defense Zone—was designed to meet the anticipated threat.<sup>13</sup>

While these historic coastal defense efforts offer lessons for command and control that will subsequently be explored, the asymmetric Global War on Terror (GWOT) threat to the nation differs considerably from the Soviet Navy. The threat is no longer against shipping per se, but rather against critical infrastructure, economic and political targets, or civilian population centers. Terrorists do not use conventional weaponry, but rather rely on asymmetric methods of attack. Modern technology has enabled terrorists to operate with a greater degree of flexibility worldwide, using sophisticated command and control techniques and weaponry. The probability of a Weapons of Mass Destruction (WMD) attack by irrational non-state actors using chemical, biological, radiological, nuclear (CBRN) and high yield explosion style weapons has increased substantially in the post 9/11 era.<sup>14</sup> These weapons' use would have a devastating impact on our economy and national psyche. In light of GWOT's asymmetric nature, however, a direct attack from the sea is not the only threat that must be considered. Using the sea to smuggle

---

<sup>11</sup> Michael Gannon, *Operation Drumbeat* (New York: Harper and Row, 1990), xviii.

<sup>12</sup> J. David Brown, "The Battle of the Atlantic: Peaks and Troughs," in *To Die Gallantly: The Battle of the Atlantic* (New York: Westview Press, 1992), 144.

<sup>13</sup> R. B. Watts, "Coastal Defense: Now More than Ever" (Annapolis: U.S. Naval Institute *Proceedings*, Dec 1990), 66.

<sup>14</sup> Sources on WMD are far more numerous after the events of 9/11. See [www.globalsecurity.org/wmd](http://www.globalsecurity.org/wmd) (accessed March 5, 2005) for one of the more comprehensive reviews of the threat.

weapons, people, illegal drugs and technologies is an age-old problem that takes on new dimensions in the Global War on Terror, and many targets that would not be considered legitimate (economic, symbolic, etc) in a conventional war now must be considered in strategic defensive planning. In short, the unimpeded use of the sea is a force multiplier for a potential enemy dedicated to striking a wide range of potential targets.

It would be inaccurate to say that prior to the attacks of 9/11 the U.S. maritime domain and activity within it were ignored by regulatory and military agencies. But the wide range of potential threats and vulnerabilities in GWOT make it apparent that a substantial increase in awareness of the maritime domain is required to ensure the homeland's security and safety. Calling for an overhaul of our intelligence systems, the National Security Strategy is specific in this regard:

Intelligence must be appropriately integrated with our defense and law enforcement systems and coordinated with our allied and friends. We must strengthen intelligence warning and analysis to provide integrated threat assessments for national and homeland security. Since the threats inspired by foreign governments and groups may be conducted inside the United States, we must also ensure the proper fusion of information between intelligence and law enforcement.<sup>15</sup>

MDA is an attempt to meet this objective by fusing law enforcement and defense intelligence into one useable, interactive information package that focuses on the maritime domain. As such, it will be inter-governmental and global in nature, considering all potential threats associated with the sea and providing this information to all agencies that can influence maritime security and defense.

## **B. WHAT IS MDA?**

In many ways, MDA is a process that institutionalizes a fundamental naval principle: before an enemy can be engaged, he must first be found. The problem is as old as warfare. Much of modern naval strategy is based on various means to locate potential enemy forces, a problem complicated by the vastness of the maritime environment, the huge number of legitimate users, and the wide variety of means by which an enemy can exploit the sea to his advantage. The oceans are complex mediums whose nature

---

<sup>15</sup> *National Strategy for Homeland Security*, 30.

provides ample opportunity for an enemy to avoid detection—weather, sea states, and coastal land masses all present considerable challenges to modern sensors. Peacetime economic use of the seas complicate this problem enormously. The oceans are the world’s foremost (and arguably most unregulated) highway, home to a vast and wide variety of international “white” (neutral or non-combatant) shipping that possess no apparent threat. Determining who or what is the enemy in such a crowded and complex environment is difficult during conventional war. During an asymmetric conflict such as the GWOT, it is almost insurmountable.

It is the asymmetric nature of GWOT that brings about the crux of MDA. In conventional naval war the enemy is relatively well defined and almost universally a combatant. The GWOT, where literally any vessel could be a potential enemy or weapon carrier, or when any maritime event can have an impact on the security of the United States, demands a much higher level of awareness than normally exercised in conventional naval conflict. This is recognized by the formal definition of MDA:

Maritime Domain Awareness is “the effective understanding of anything associated with the global maritime environment that could impact the security, safety, economy or environment of the United States. This is accomplished through the integration of intelligence, surveillance, observation, and navigation systems into one common operating picture (COP) that is accessible throughout the U.S. Government.<sup>16</sup>

There are several key points in this definition that bear close examination. Unlike traditional naval operations, it is apparent that the goal of MDA is far more than simply looking for potential maritime enemies poised to attack the United States. “Anything associated” with the maritime environment that can impact (not necessarily threaten) the security, safety, economy or environment goes far beyond what many would envision as a classic maritime threat. These include smuggling of people or dangerous cargoes, piracy, proliferation of Weapons of Mass Destruction (WMD), identification and

---

<sup>16</sup> *National Security Presidential Directive 41* (Washington D.C.: The White House, December 2004), 13.

protection of critical maritime infrastructure, oil spills, weather, and environmental concerns among other events. These elements and a host of others must be considered to achieve true MDA.<sup>17</sup>

Maritime events that could potentially impact the United States are not the only wide-ranging element of MDA. HSPD 13 requires that threats be identified as early and far from our shores as possible. Because of this requirement, MDA is not a homeland centric process; rather, it is *global* in nature. Because of the potential impact to homeland security, activities occurring overseas and in foreign ports are very much a part of MDA. For example, if a cargo is loaded in Singapore and its ultimate destination is the United States (via several other international ports), the loading, transport, security, and all matters associated with that container would be part of MDA. MDA must therefore be exercised over all oceans worldwide, and potentially cover all maritime interests that ultimately deal with the United States.

The range of potential security challenges and enormous geographic area represented by the maritime domain makes achieving anything close to effective MDA a huge undertaking. This was recognized early in planning for its implementation. MDA was originally conceived as a Coast Guard concept in the late 1990s to track various “Special Interest Vessels” globally. After 9/11, it was realized that this application could be expanded to include all actions in the maritime domain of potential threat to the United States.<sup>18</sup> Although the Coast Guard was the Lead Federal Agency (LFA) for MDA, it was never conceived as a Coast Guard centric program. Early in the concept development process Coast Guard leadership formed a strong partnership with the Navy in planning and use of assets. During an “MDA Summit” held at the Secretary level in May 2004, Mr. Paul McHale (Assistant Secretary of Defense, Homeland Defense) and Admiral James Loy (Deputy Secretary Homeland Security), with the concurrence of Secretary Rumsfeld and Secretary Ridge, brought together senior members of 16 respective Departments and Agencies involved in some degree with the maritime domain. The ultimate goal was to devise a plan for these agencies to work together for both

---

<sup>17</sup> CONOPS, 1.

<sup>18</sup> High interview, 25 March 2005.

implementation and continued execution of MDA. The stated goal of this summit was to coordinate a compilation of diverse information into one common, usable format that could be accessed by all the agencies involved in the maritime domain.<sup>19</sup> Ultimately these Agencies formed a Senior Steering Group (SSG) specifically to accomplish these objectives through the drafting of the MDA Strategy.

These agencies possess a wide range of operational and intelligence capabilities that require some degree of fusion under the over-arching goal of MDA. Fusion of these capabilities is key. The overall goal of MDA is noble, but extremely ambitious. For true MDA to be achieved, a process has to be defined which best leverage the various multi-agency capabilities that are able to contribute to that process. These actual mechanics of MDA are based heavily on established naval principles for maritime surveillance.

### C. MDA: THE MECHANICS

Effective MDA is more than simply agreeing that various government agencies will cooperate in ocean surveillance. It is a process that attempts through a broad awareness to properly identify threats for appropriate action. As such, MDA borrows heavily from established naval principles and previously established coastal defense models. In traditional naval combat, a threat must first be detected, localized, classified and targeted before it can be effectively engaged. Although many factors are considered in MDA, its core process is ultimately the monitoring of vessels and the vessels' cargo, crews, and passengers to rapidly generate geo-locating information on vessels of interest. This is an analytical process that includes tracking, data base searches for unknown linkages and anomaly detection. Fundamental to this is the detection, monitoring, and

---

<sup>19</sup> Statement of Mr. Jeffrey High on the U.S. Coast Guard's MDA Efforts before the Subcommittee on Coast Guard and Marine Transportation Committee on Transportation and Infrastructure, U.S. House of Representatives ([www.house.gov/transportation/cgmt/10-06-04/high.pdf](http://www.house.gov/transportation/cgmt/10-06-04/high.pdf), October 2004, accessed September 10, 2005), 5.

tracking of vessels. This tracking process is comprised of five components designed to narrow a wide area surveillance to an area of tactical dimension where threats can be identified and isolated:<sup>20</sup>

- **Surveil.** Maritime surveillance is the observation of activity in all areas and environments within the Area of Interest (AOI) or Area of Responsibility (AOR). It is multi-dimensional, including aerospace, land, sea surface, and undersea environments.
- **Detect.** Detection is dependent upon the capability and employment of sensors and/or intelligence. Detection of maritime activity or potential threats is the first indication that some form of response or defensive action is required. Specific intelligence may direct sensors to concentrate in an area to detect a particular Target of Interest (TOI).
- **Track.** Tracking is the display or recording of the successive positions of a moving object. Tracking must be maintained to allow decision makers to achieve an end result that is mission and situation specific, including doing nothing, monitoring, interdicting, or eliminating the threat or challenge.
- **Classify and Identify.** Classification and Identification is the determination of a characteristic or set of characteristics that uniquely differentiates a particular vessel, target, or event from others in the same classification category. This information is often correlated through the use of intelligence, analysis and information databases.
- **Target.** Targeting involves interpreting detection and identification information fused with intelligence to sort vessel intentions and determine risk. Targeting involves evaluating detected vessels and determining which possess unresolved risk from activity, intelligence, and anomalous behavior.

This process is illustrated in Figure 1<sup>21</sup> below:

---

<sup>20</sup> *Concept of Operations (CONOPS) for Maritime Domain Awareness*, Version 1.28 (Washington D.C: U.S. Coast Guard, 30 September 2004), 6.

<sup>21</sup> Ibid.

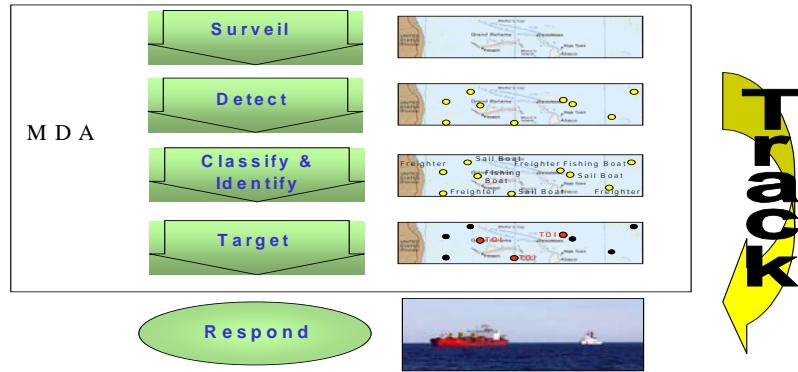


Figure 1. MDA Tracking Process

MDA's core is applying the vessel tracking process to a layered defense model centered on the coastline of the United States, the ultimate goal of which is to detect potential threats early and as far away from the U.S. coastline as possible. Layered defense is a classic navy tactic applied to battle group operations to protect a "high value unit" (HVU) such as an aircraft carrier. In the past this layered defense model has been applied to coastal defense for conventional conflict. In that particular case, the "high value unit" is generally considered the port or facility vital for military operations.<sup>22</sup> There are key differences, however, in the layered defense used in the classic military model and MDA. As there is no single high value unit per se, MDA "layers" are expanded to include an entire coastline with the overall goal of coordinated surveillance. Not all areas in these "layers" are considered equally, but rather additional attention is given to areas that are potential targets for our terrorist enemy.

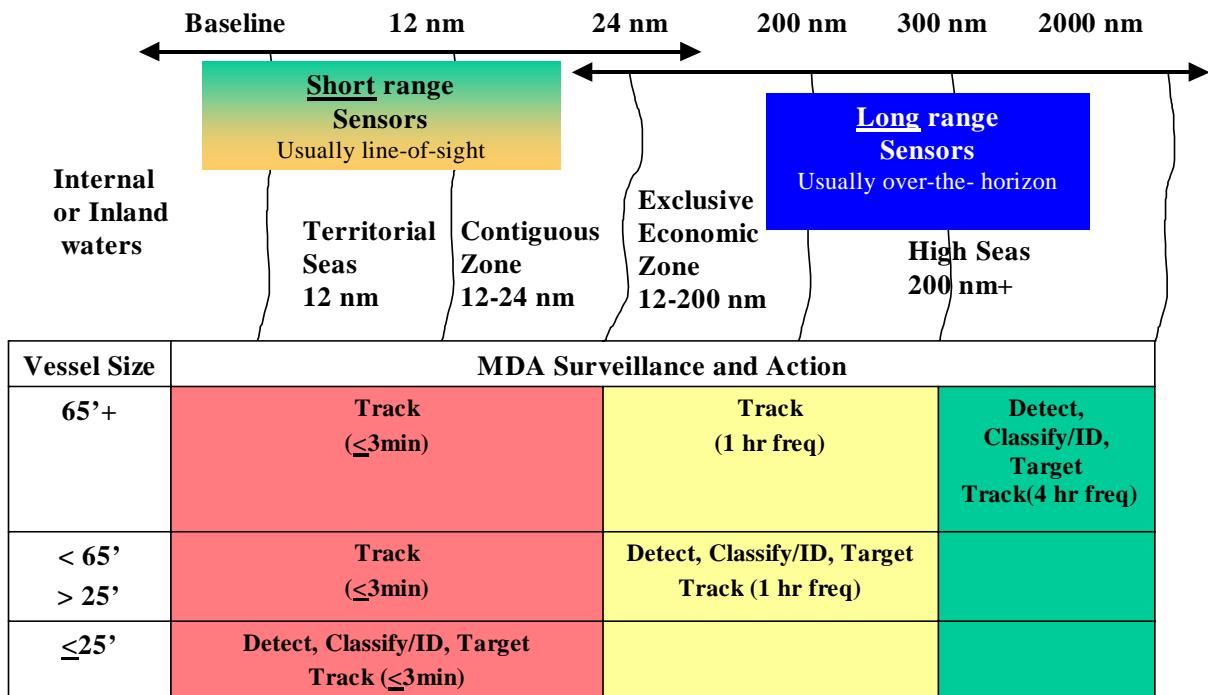
Layered defense in MDA terms is represented by a Maritime Detection and Identification Zone (MDIZ). The MDIZ places a high degree of emphasis on timeliness of detection and tracking of ALL vessels. Since the threat is asymmetric and often uncertain all vessels are subject to the surveillance process, requiring an improved timeliness of tracking as vessels get closer to U.S. waters (Figure 2).<sup>23</sup>

---

<sup>22</sup> R.B.Watts, "Defending Our Shores" (Annapolis: U.S. Naval Institute *Proceedings*, Oct 1987), 42.

<sup>23</sup> CONOPS, 8.

# Maritime Detection & Identification Zone



MDIZ constructed based on capabilities of existing and projected sensors, and the operational commanders' need to develop and execute a response for each target class.

Figure 2. MDIZ

The 2000nm limit of the proposed MDIZ is based on the recently legislated 96 hour notification requirement for foreign vessels entering U.S. ports. A vessel traveling 20kts will arrive at its destination in roughly 96 hours.<sup>24</sup> As shown in Figure 2, the MDIZ's goal is to gather more timely information on the vessel as it approaches closer to the U.S. coast. When entering the MDIZ, positions every four hours are the norm while in territorial sea the goal is to obtain positional data every 3 minutes, recognizing that as a vessel gets closer to a potential target the greater potential threat it represents.

<sup>24</sup> The 96 hour notification requirement was mandated by the Coast Guard in the wake of the 9/11 attacks. Note, however, that this is only a requirement for vessels entering U.S. ports, not vessels engaged in innocent passage. The MDIZ is not in any way a regulatory zone, but rather intended as a guideline for detection parameters. Ibid., 7.

MDA's objective is to create a continuous awareness that utilizes a layered defense model to identify potential maritime threat. But how can it be implemented? In theory, all maritime activity will be tracked within the MDIZ for potential response. As noted in the projected requirements, however, MDA's actual practice is complex. Who will execute the surveillance process or monitor activity in the MDIZ in the multi-agency environment is unclear, especially given the wide range of capabilities that apply in the maritime domain. Although the concept of MDA as information is clear, how this information will be collected, analyzed, and disseminated or who will maintain overall authority over the MDA remains to be developed. These and other questions require a defined organizational construct that reaches across the three levels of MDA execution: tactical, operational, and strategic.

### III. MDA ORGANIZATIONAL CONSTRUCT

MDA's core objective is obtaining awareness through a layered defense. On the surface, the solution to this problem would seem fairly straightforward. As we have divided the ocean into various "zones," simply assigning a large number of various sensors to these zones would seem to solve the problem of overall surveillance and vessel tracking.<sup>25</sup> Unfortunately, the problem is far more complex. While there are many potential systems that could provide a high degree of surveillance and tracking data, the actual *fusion* of this data remains problematic. Information that cannot be correlated and analyzed is simply information for information's sake. In order to derive a comprehensive MDA picture, information must be fused, correlated, and analyzed. This requires an organizational construct.

It is obvious from examining the theoretical MDIZ that MDA, and the subsequent organizational architecture that will execute it, must be approached from a number of levels. While a port command may exercise excellent tactical control within its sphere of influence, for example, this is naturally limited by available sensors, forces, and geography, so events occurring 2000nm offshore are all but invisible. Similarly, a port's day-to-day operations will be largely invisible to a command center dedicated to coordinating fleet movements in ocean areas or worldwide. Both are arguably part of MDA, demonstrating the need for a logical division of labor to coordinate all levels into one comprehensive picture.

In traditional military theory, warfare is conducted on 3 respective levels: Tactical (operations of individual or small groups of forces), Regional/Operational (operations of large groups of forces or fleets), and Strategic (operations on a theater or national level).<sup>26</sup> To be effective an MDA organization must be designed to operate on each of

---

<sup>25</sup> In experiments conducted by the Coast Guard in coastal maritime surveillance, it was found the addition of multiple sensors actually complicated the MDA problem enormously. Without fusion, correlation and analysis of sensor information each track had to be individually verified, a tremendous drain on operational resources. Fusion of data attempts to limit this trend by detection of anomalies. "Fusion and MDA Systems," ONR brief to the Assistant Secretary of the Navy, 31 March 05.

<sup>26</sup> *Department of Defense Dictionary of Military and Associated Terms*, Joint Pub 1-02 (Washington D.C., Government Printing Office, 12 April 2001), 419, 311, 406.

these levels in different ways that remain linked to provide one overall comprehensive picture. On the tactical level, MDA supports on-scene decision makers and focuses on tracking an immediate threat. Day-to-day operations in ports and activities immediately offshore become the focal point at this level. On the regional level, MDA information is analyzed within the context of activities along an entire coast, while the strategic level focuses on activities overseas and uses information obtained from the tactical and regional levels to conduct long term planning or tactical and operational activities against specific threats overseas.<sup>27</sup> Each level is crucial to overall MDA and will be examined in turn.

#### A. TACTICAL MDA

It is a fundamental theory of DHS that effective homeland security is conducted on a local or tactical level. Much of the HLS effort subsequently focuses on local operational forces and first responders.<sup>28</sup> Through the vigilance of law enforcement, it is here that a potential threat is often initially detected and neutralized. In terms of HLS MDA, the tactical level focuses on ports and the maritime “approaches” to the United States—in this case defined as 30-40 miles offshore.<sup>29</sup> While these zones have always been high areas of focus for maritime security operations, post 9/11 these operations have changed considerably as a result of Coast Guard and Navy response to an asymmetric terrorist threat. An examination of this change is crucial for an understanding of tactical MDA.

Prior to 9/11 the Coast Guard port and offshore tactical construct was divided into two separate areas of responsibility. In major ports the traditional “Captain of the Port” (COTP) position was assigned to a respective Marine Safety Offices (MSOs) responsible

---

<sup>27</sup> *National Plan to Improve MDA*, First Coordination Draft, March 2005, 5.

<sup>28</sup> This underlying assumption has been key to a number of DHS decisions, including President Bush’s nomination of NYPD Police Commissioner Kerik to lead the Dept. See “All Homeland Security is Local,” *Slate*, Dec 3, 2004, accessed February 19, 2005.

<sup>29</sup> The actual definition of “approaches” varies considerably. To date, there is no standard definition in Joint or Service doctrine; in operational planning, however, it is generally considered that “approaches” in the tactical sense is defined as the effective operating range of sensors and response capability of tactical assets. See “Technology Working Group Briefing, MDA.” USCG Innovation Expo, San Diego CA, 2 May 2005.

for regulatory functions, such as vessel inspection, environmental response, licensing, etc. COTPs were (and are) responsible for merchant vessels entering and leaving port, coordinating vessel inspections for maritime safety, and coordinating incident response. Maritime law enforcement conducted by MSOs was distinctly regulatory in nature—many vessel inspectors and recreational boating safety personnel performed their duties unarmed. Operations of a more traditional, law enforcement variety, such as counter-narcotics or fisheries enforcement, search and rescue and other offshore operations were the responsibility of a “Group” that maintained command and control of subordinate “Stations” in the Area of Responsibility (AOR) assigned that Group.<sup>30</sup> While this description is admittedly overly simplistic, it would be fair to say that MSOs “owned” the ports and all responsibilities for large merchant vessel and container operations that traditionally required regulatory attention, while Groups focused offshore and conducted law enforcement operations dealing with smaller maritime traffic or search and rescue. Afloat operational assets (utility boats, patrol boats, and small cutters) were generally “owned” by the groups and used offshore in traditional law enforcement, although there was limited cooperation with the MSO for close inshore operations that required these assets.<sup>31</sup>

While this relationship and division of responsibility made sense prior to 9/11, the new asymmetric threat altered the equation considerably, requiring a merging of traditional responsibilities across established lines of command. The expanded threat spectrum now reached directly into the ports. Pure regulation, although still important for security, no longer sufficed. A direct law enforcement response capability (traditionally the role of Groups) was now required in the ports. Alternatively, tracking and intercept of large merchant vessels, traditionally an MSO function, took on a new

---

<sup>30</sup> The composition of Groups varies considerably. Traditionally, Groups were composed of a command center and had direct control of a number of smaller afloat assets, such as patrol boats and buoy tenders, and occasionally were co-located with air stations and controlled the helicopters/planes assigned to that station. “Stations” were smaller CG commands that maintained small offshore utility boats for near coastal SAR and law enforcement. Author’s operational experience. See also P.J. Capelotti, “The Coast Guard’s Response to 9/11,” *Joint Center for Operational Analysis and Lessons Learned*, Vol VI, Issue 4, September 2004.

<sup>31</sup> Each Group/MSO had individual Standard Operating Procedures (SOPs) that detailed this relationship, which varied in individual ports. The characterization/summary of these relationships is based on the author’s operational experience.

meaning as these vessels potentially represent a threat to the security of the United States. Subsequently, merchant vessel regulation focusing on maritime security was “pushed” far offshore with the establishment of a layered defense.<sup>32</sup> The new threat also affected other agencies with maritime security concerns. Ports with high Navy interest such as Navy bases, research facilities, critical infrastructure, and out load responsibilities augmented traditional security with extensive anti-terrorist force protection (ATFP) procedures to prevent, among other things, a “USS COLE” style attack on potentially vulnerable warships. U.S. Customs immediately implemented increased forms of container and cargo security measures that were completely lacking prior to 9/11. These new multi-agency security requirements demand revamping the traditional dual track and somewhat laissez-faire command system exercised in U.S. ports prior to 9/11 will no longer suffice.

Internally, the Coast Guard’s response to the new threat was a merging of responsibility under a newly designed “Sector” organization, an effective combination of MSO and Group responsibilities and assets. The Sector has sole responsibility for all Coast Guard missions in one geographic area.<sup>33</sup> This significant re-organization was an important first step within the Coast Guard that soon took on a multi-agency nature. The Coast Guard reinforced traditional close ties to other port agencies in the design of Sector Command Centers (SCCs) that included multiple organizations. The link to DOD was made through a specialized SCC called the Joint Harbor Operations Center (JHOC), an experimental fusion center that quickly demonstrated its utility in providing tactical MDA.<sup>34</sup> Recognizing a mutually beneficial interest in coordinating operations, the first JHOCs focused on fusing Coast Guard and Navy operations in port protection and ATFP

---

<sup>32</sup> *Maritime Strategy for Homeland Security* (Washington D.C: U.S. Coast Guard, July 2002).

<sup>33</sup>Where applicable, Sector organizations also include Vessel Traffic Services (VTS) and CG Air Stations. CONOPS tab a, a-5-a-1.

<sup>34</sup> Note that the term “JHOC” is technically not accurate. At the time of this writing, Sector Command Centers (SCCs) with USN participation are designated “SCC-J” (Joint)—the term JHOC, however, is widely recognized in DOD and will likely to remain in the lexicon for some time. For this reason, JHOC and SCC-Js will remain synonymous throughout this paper. Additionally, many SCCs are not designed with a Navy component, yet still link with other agencies involved in MDA. For this reason, the current infrastructure model considers all SCC types tactical components of MDA. See Dana Goward, “Unclassified Briefing to Maritime Security Integration Group (MSIG),” Pentagon, Feb 28, 2005.

where the Navy had a large fleet presence.<sup>35</sup> Given their multi-agency approach to port security and littoral operations, JHOCs are a natural choice for the implementation of tactical MDA.

JHOCs are far more than a merging of CG traditional roles and responsibilities with USN security procedures. Coast Guard and Navy cooperation is neither new nor particularly unique. Since the earliest days of each organization, both have used similar equipment and procedures in order to effectively operate together during time of war. But despite overseas operations in GWOT, U.S. ports are not on a war footing. Rather, commerce and port operations continue at the normal pace, albeit under increased security procedures. Recognizing the number of agencies that operate in ports and the vast information requirements to obtain true MDA, an effort was made to make JHOCs truly inter-agency by providing linkage to these agencies, including the establishment of formal liaison positions and data sharing protocol, with the goal to merge regulation, law enforcement, and anti-terrorist force protection data and procedures.

The first experimental JHOCs were constructed and successfully tested in San Diego and Norfolk, ports that represented high strategic interest due to major Navy presence and the volume of overseas commercial traffic. These JHOC's multi-agency design was based on previously established relationships the Coast Guard had established during its normal operations within each port. This is illustrated in Figure 3 below:<sup>36</sup>

---

<sup>35</sup> It is important to note that at the time of this writing DOD participation in JHOCs are limited to ATFP, so USN presence in JHOCs are currently limited to areas of fleet or asset concentration. "JHOC Working Group Meeting/Briefing to Maritime Security Integration Group", Pentagon, 22 June 2005. It is a core recommendation of this thesis that this participation be expanded to include MDA.

<sup>36</sup> "Pacific Area Capabilities and Interoperability for Homeland Security/Homeland Defense," (Alameda: Unclassified briefing to Honorable Paul McHale, December 14" 2004).

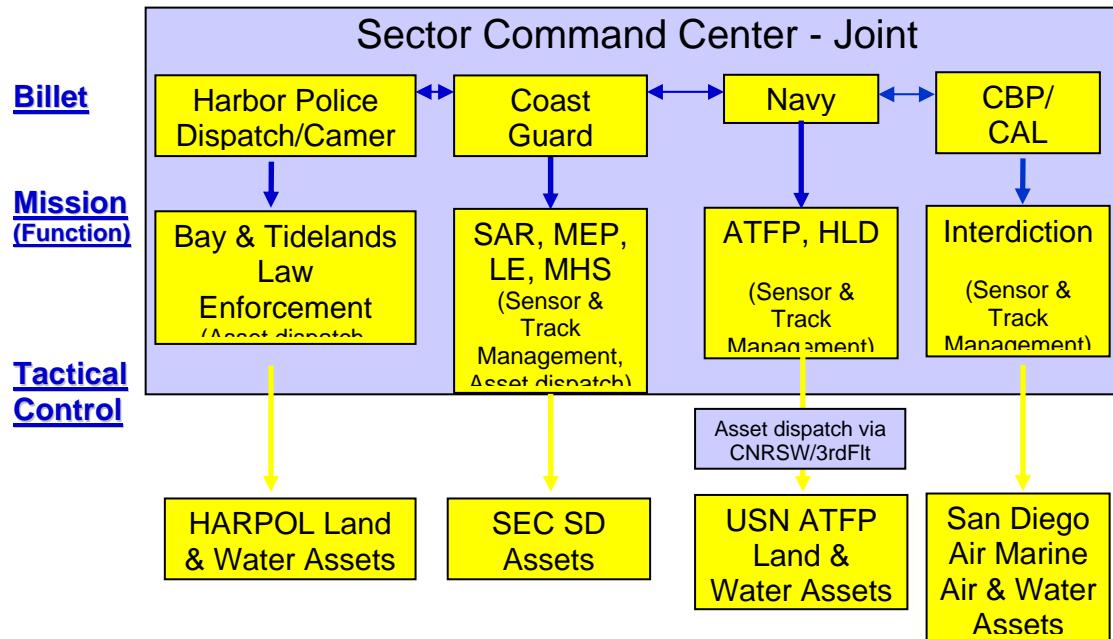


Figure 3. Sector Command Center Structure

JHOCs possess several unique capabilities that contribute significantly to tactical MDA. As command and control centers for ports and their immediate vicinity, JHOCs have inherent surveillance capability that can contribute to a COP. Using the San Diego JHOC as an example, these systems include:

- USCG Coastal Radar
- USN Port control/offshore radar system
- Automated Identification System processors
- San Diego port control camera system (civilian)
- Navy waterside security system
- Border patrol camera/thermal imagery system

JHOCs can serve as the critical fusion point for various intelligence data bases of agencies participating in the JHOC. These data bases currently include the Coast Guard's

Maritime Information Safety and Law Enforcement system, the Automated Regional Justice Information System (Naval Criminal Investigative Service), and intelligence from the local Joint Terrorism Task Force.<sup>37</sup> Through the use of inter-agency sensors and local inter-agency liaison, the JHOC effectively collects, fuses, and disseminates information that is critical for achieving tactical MDA.

Although there are only two fully functional JHOCs today, their developing construct serves as a model for a future development. This is especially true in the area of multi-agency liaison. In addition to acting as a fusion center for multiple data bases and intelligence, one of the great advantages of a JHOC structure is its joint personnel structure. Although primarily manned by Coast Guard personnel, billets are established from all agencies that have port responsibility, representing a unique merger of personnel with regulatory, law enforcement, and military expertise.<sup>38</sup> This liaison system is fundamental to the success of tactical MDA not only for coordination of operations, but also to reach an understanding of multi-agency procedures and practices. Given the large number of regulatory agencies operating in each port, there are a number of procedures specific to each agency that can have critical impact on other multi-agency operations. Customs container inspections, for example, is a critical part of vessel tracking and re-routing performed by the Coast Guard; FBI tracking of potential terrorist suspects a key element of ATFP for the Navy and facilities security forces. This type of information, and perhaps more importantly, how these procedures are carried out can be provided immediately by effective liaison that effectively merges different agency operations into one efficient cooperative effort.

---

<sup>37</sup> Goward, MSIG brief, Pentagon, 28 Feb 2004.

<sup>38</sup> "Maritime Intelligence Fusion Center Capabilities and Operations," briefing to author, December 2004.

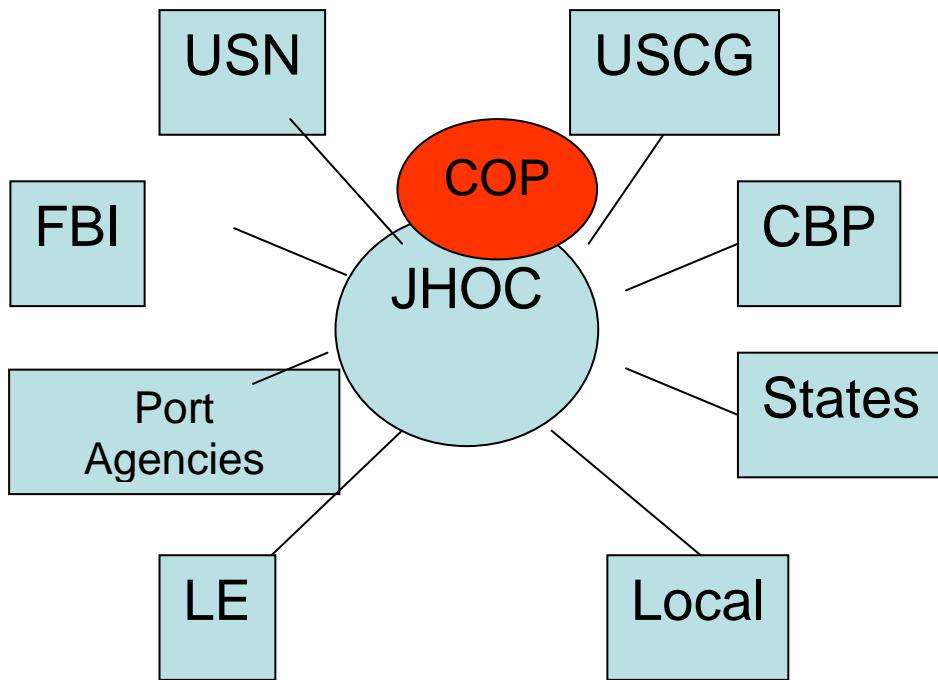


Figure 4. JHOC/COP

Figure 4 above illustrates the number of potential agencies or groups that can contribute directly to a JHOC and share in the Common Operational Picture (COP) to achieve tactical MDA

JHOC San Diego's and Norfolk's initial successes led to a joint Coast Guard-Navy study to expand the project to other ports of strategic interest. Ports with Navy presence, high commercial infrastructure, and 'outload' capability (loading of wartime material and supplies critical for overseas efforts) were considered for JHOC installation.<sup>39</sup> Today there are 6 high priority ports being upgraded to JHOC status, and approximately 17 SCCs that are being considered for some form of future upgrade for USCG-USN integration.

Multi-agency JHOCs offer several advantages for the effective implementation of tactical MDA. In the post 9/11 construct, JHOCs and SCCs were initially designed as natural combinations of port command and control activity operating outside of the realm of tactical MDA. But seen as part of the greater picture, their application to MDA is

---

<sup>39</sup> Goward, MSIG brief, Pentagon, Feb 28, 2005.

obvious. By acting as combined, multi-agency fusion centers they provide a unique tactical picture that all MDA users can employ at the port level. This increased multi-agency awareness provides for streamlined operations between all port agencies, while the use of multi-agency sensors and data bases allows for a tremendously enhanced capability for surveillance and anomaly detection. Additionally, the critical fusion function performed by the JHOCs allows tactical information to be entered into a COP that can be accessed by MDA users in the regional and strategic spheres, the first step in obtaining a larger, regional picture and ultimately achieving strategic MDA.

## **B. REGIONAL/OPERATIONAL MDA**

Joint inter-operability at the tactical level is an important first step in obtaining MDA, but by itself cannot obtain the overall goal of global maritime awareness. Tactical homeland security quite rightly centers on the ports and their immediate approaches. To achieve MDA, this information must be viewed as part of an overall whole, not only to ensure proper coordination between assets, but also to extend the “reach” of domain awareness to detect potential threats as far from the homeland as possible. This is MDA’s role on the operational or regional level.

The operational/regional level of coordination is generally considered to occur at a “fleet” or “agency” level—in terms of the Coast Guard or Navy, for example, this focuses on District/Area command, or Fleet commander level respectively. FBI, Customs, and other DHS agencies all have roughly equivalent layers of command or bureaucracy that coordinates tactical or field operations at this level. In response to the 9/11 attacks, many intelligence watches or fusion centers were “stood up” to coordinate the new requirements of GWOT and homeland security adding to intelligence centers already in existence that refocused their efforts toward the terrorist threat. The purpose, function, and focus of these various fusion centers vary considerably. Designed to meet the need of their parent organizations, most formed using compartmentalized information and procedures.<sup>40</sup> In the maritime arena, these centers/groups include, but are not

---

<sup>40</sup> Mark Stevens, “*As Is*” National Maritime Domain Protection System (Monterey: Maritime Domain Protection Research Group, November 2004), 28.

limited too, Fleet/ Combatant Commander (COCOM) Staff N2s (intelligence), Joint Inter-Agency Task Force components, Naval Criminal Investigative Service (NCIS) offices, Coast Guard District Intelligence, and Custom Border Patrol (CBP) offices, and Federal Law Enforcement centers.

While each group possesses their own unique area of focus and expertise, none is exclusively directed specifically toward MDA. As the lead federal agency for MDA implementation, it follows that the Coast Guard should be the agency to bring these groups together in one fusion center/COP specifically for MDA. As the JHOC did on the tactical level, the Coast Guard can perform this function with infrastructure currently in place, using the newly created Maritime Intelligence Fusion Centers, or MIFCs.

MIFCs were created specifically to deal with the increased intelligence requirements of the maritime homeland security mission. Organizationally, Coast Guard operational forces on each coast are commanded by a CG fleet commander equivalent, Coast Guard Atlantic Area (CGLANTAREA) in the Atlantic and Coast Guard Pacific Area (CGPACAREA) in the Pacific. Prior to 9/11 these commands linked with various Navy and law enforcement intelligence agencies to provide specialized forms of intelligence (military, counter-narcotics, etc) for use by operational forces. While this intelligence was used for strategic and operational purposes, this was generally focused on traditional USCG law enforcement missions. The counter-terror missions required post 9/11 increased these intelligence requirements exponentially, necessitating the creation of MIFCs at each Coast Guard Area to provide direct intelligence support to the Area Commander, specifically to deal with operational intelligence and coordination of MDA-like activities.

MIFCs are far more than staffs. Possessing over 50 intelligence specialists and analysts, MIFCs collect, analyze and disseminate operational intelligence, both to tactical units in the field and strategic fusion centers up the chain of command. MIFCs have access to national intelligence, law enforcement intelligence, and subject matter experts in the intelligence community. In addition to providing intelligence analysis, MIFCs are capable of deploying experts, equipment, and sensors to support tactical operations when

required.<sup>41</sup> In their formal charter, MIFCs focus on regional homeland security, migrant interdiction, counter-drug operations, defense readiness, living marine resources (LMR) enforcement, and search and rescue—all components of MDA.<sup>42</sup>

MIFCs serve as a collection point for tactical intelligence, but also provide a key analytical function that is lacking at the tactical level. This is a critical point; although JHOCs certainly provide a low level of analysis on local information, this is by necessity extremely tactical and very limited, as there are no personnel specifically dedicated to the analytical role. By its regional nature and access to a broad amount of information from tactical and strategic sources, MIFCs have the ability to support tactical operations and piece together parts of an overall intelligence picture. Dedicated personnel at MIFCs perform both short and long term analysis that is critical for planning and response. Through its connection to tactical and strategic levels of command, the MIFC can provide product both up and down the chain of command for immediate tactical use as well as further strategic analysis. Specifically, this regional analysis focuses in the following areas:

--Collection/Ops Management: MIFCs act as a focal point for collection of field intelligence, not only from operational Coast Guard units but also multi-agency partners operating in ports in the AOR.

--ELINT fusion: MIFCs possess an electronic intelligence component that collects and fuses electronic information to supplement other intelligence sources.

--Combatant Commander Level: As a COCOM level unit, MIFCs liaison with local USN fleet commanders to share maritime intelligence, fusing this information in one common product.

--Coordinated Operational Intelligence Production: MIFCs produce a number of intelligence support products, including tactical products for use by field units (daily

---

<sup>41</sup> Stevens, “*As Is*” National Maritime Domain Protection System, 21.

<sup>42</sup> “Maritime Intelligence Fusion Center Capabilities and Operations,” Briefing to author, Dec 2004.

intelligence summaries, ATFP reports, Alerts/Advisories, and management of a common intelligence picture), and operational/strategic reports and analysis based on input from the field.<sup>43</sup>

These analytical functions represent the first real step from local, responsive tactical MDA to a broader effort to obtain a wider area picture, and begin the trend analysis that is vital for overall awareness and anomaly detection.

Although designed and staffed by the Coast Guard, MIFCs exercise a “joint” nature that is particularly valuable for an MDA construct. MIFCs were designed specifically to fuse and analyze the vast amount of joint and multi-agency information and intelligence that affects the maritime domain. To link directly with Navy activities, MIFCs are co-located with Navy Shipping Coordination Centers (NSCCs). Originally designed to warn Navy ships of merchant ship activity that might interfere with ongoing operations, NSCC now provides information to MIFCs that allow them to identify shipping anomalies or suspicious commercial vessel activity. In addition, MIFCs have established interagency liaisons with the Immigration Customs Enforcement (ICE), Customs Border Patrol (CBP), National Security Agency (NSA), Federal Bureau of Investigation (FBI), USN COCOMs, and strategic intelligence sources. Using the unique Coast Guard’s dual law enforcement/military nature of the CG, MIFCs serve as a collection, fusion, and analysis point for both law enforcement and military intelligence data.<sup>44</sup>

The diagram below details liaisons currently in place at MIFC PAC:

---

<sup>43</sup> “Maritime Intelligence Fusion Center Capabilities and Operations,” Briefing to author, Dec 2004.

<sup>44</sup> The sharing of law enforcement and military intelligence is not universal; due to restrictions imposed by U.S. law, the types of information that can be fused in these two areas that are available to all agencies is limited. See appendix 2.

## **PACAREA MIFC Intelligence Partners:<sup>45</sup>**

| <b>LAW ENFORCMENT</b>   | <b>DOD/INTELLIGENCE CENTERS</b>       |
|---|---------------------------------------|
| Department of Homeland Security   | NORTHCOM Intelligence Watch           |
| “Legacy” Customs, ICE/CBP Intelligence Coordination Center (USCG)       |                                       |
| Joint Terrorism Task Forces (JTTF)                                      | MIFC Atlantic                         |
| Coast Guard Investigative Services                                      | National Maritime Intelligence Center |
| Air Marine Operations Center  | Joint Intelligence Center Pacific     |
| California Anti-Terrorism Info Ctr                                      | Commander Third Fleet Battle Watch    |
| El Paso Intelligence Center (EPIC)                                      | Canadian Maritime Forces Pacific      |
| Royal Canadian Mounted Police   | NOPF Whidbey Island                   |
| Joint Inter-Agency Task Force South Defense Intelligence Agency/JIFT-CT |                                       |
| Coast Guard Operational Cmds  | National Security Agency              |
| CIA/Terrorist Threat Integration Center                                 |                                       |

The wide range of maritime intelligence available to the MIFCs for both tactical dissemination and operational analysis make them a natural fusion point for regional/operational level MDA. As regional commands they can be key interface between tactical centers (JHOCs). This is illustrated in Figure 5.

---

<sup>45</sup> Goward, MIFC brief, Pentagon, Feb 28, 2005.

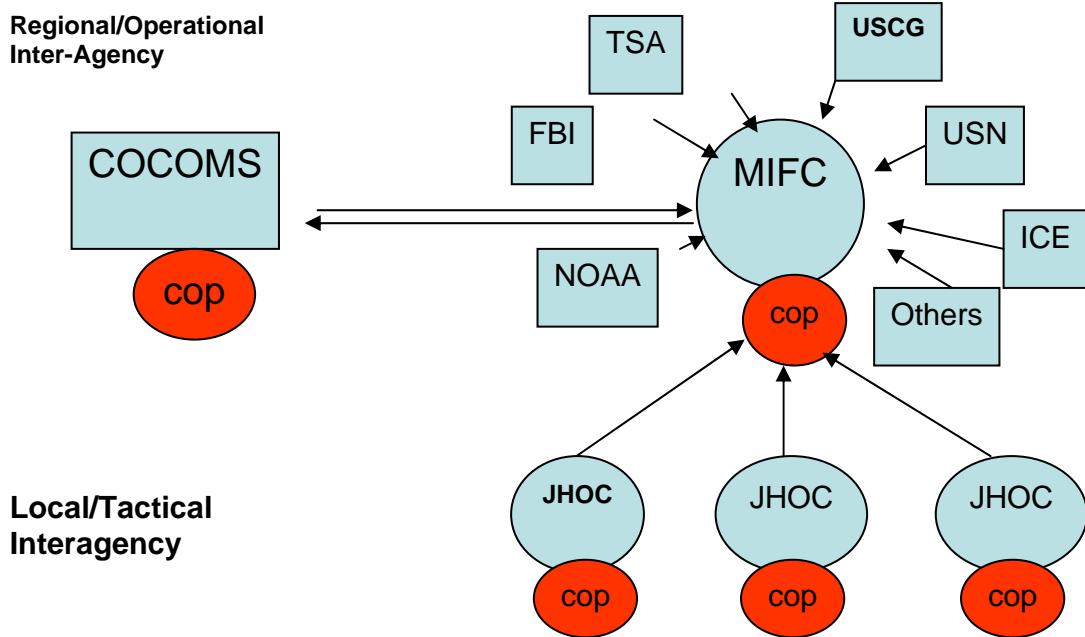


Figure 5. MIFC

MIFCs are not the only regional command center that focuses on maritime intelligence. As noted, most agencies maintain some form of regional operations center, as do applicable COCOMs. But these centers are naturally focused in their individual areas of expertise, whereas the inherent design of MIFCs was intended to be multi-agency in nature. The Coast Guard's unique position vis a vis DOD and DHS is also an important factor. As a military service the Coast Guard maintains the same equipment and reporting procedures as DOD, while their Title 14 (law enforcement) authority provides a natural link to other law enforcement and civilian regulatory maritime agencies. This “dual hatted” nature, as well as a long standing familiarity with the area of operations, make MIFCs a natural choice to be the fusion point for regional MDA.

Like all elements of MDA, fundamental to the success of MIFCs will be the development of a multi-agency electronic COP and the establishment of multi-agency liaison officer positions at each MIFC. This liaison element is especially important on the regional level. While tactical operations at JHOCs will rely on established local relationships, decisions and analysis on the MIFC level require in-depth knowledge of policies and procedures from all participating agencies. MIFCs are the first analytical

level of MDA, and as such require considerable cooperation across agency lines to ensure comprehensive analysis is conducted. Manning MIFCs with appropriate level inter-agency subject matter experts is therefore critical for a comprehensive regional picture that can be shared with both JHOCs on the tactical level, and national decision makers on the strategic level of MDA.

### C. STRATEGIC MDA

Traditionally strategy drives doctrine, procurement and ultimately field operations. Ideally, all levels of the command or organization are responsible for executing some part of the strategy, while providing lessons learned which can be used to modify the strategy accordingly. Strategy sets the course for the organization and the operations that follow, and as such is critically important for overall success. On the national level, strategy is critical for long term planning, operational insight, and providing national decision makers with support to establish priorities, determine agency strategies, allocate national resources, and determine level of overall maritime threat.<sup>46</sup> This is a difficult process during normal peacetime operations and is particularly challenging in the constantly changing asymmetric maritime environment that MDA is designed to address.

MDA's ultimate goal is to obtain a sense of global awareness that reaches beyond the confines of the tactical and regional levels. Were MDA simply a defensive strategy against a known military or terrorist threat, it could arguably be obtained simply by forming defensive layers around the United States. But as an informational/awareness system, its goals are far broader, seeking to understand all potential maritime threats to the homeland, many of which could originate overseas in the most innocuous of manners. It is the obtaining of vital bits of information and piecing together the puzzle that true MDA is achieved, and this requires a global outlook. Global maritime awareness is the core of MDA and is widely recognized in a number of national strategies that deal with the terrorist threat. These include the National Strategy for Maritime Security, the National Security Strategy, the National Strategy for Homeland Security, and the

---

<sup>46</sup> *National Plan to Improve Maritime Domain Awareness*, 5.

National Strategy to Combat Weapons of Mass Destruction.<sup>47</sup> These strategies rely on MDA as both an enabler and force multiplier to their individual core objectives. Without an implemented strategic MDA, many of the basic tenets of these strategies will remain unfulfilled and unobtainable.

Obtaining true global and strategic awareness is one of the most difficult objectives of MDA. While linking tactical and operational MDA capabilities can effectively provide a picture of ports and much of the mid-ocean regions, this is decidedly homeland centric and far more operational in scope than a global or strategic picture. Strategic MDA requires a detailed multi-agency linkage on a level that is far more complex than the simple linking of JHOCs and MIFCs. The size and scale of this effort is problematic. MDA is unique among government programs in that it is truly multi-agency, its scope reaching far beyond normal bureaucratic experience. Strategic MDA requires the realignment of bureaucracy and the re-tasking of national assets toward the overall goal of global awareness. This requires a huge cultural change that presents a host of new difficulties, not the least of which is the requirement for a large number of civilian and military agencies with entirely different policies and procedures to cooperate together more clearly than they ever have before, toward one common goal.

Strategic MDA requires a broad perspective and capabilities at the highest levels of analysis, intelligence, and policy. Since strategy and overseas operations are inherently a function of the military services, it would seem that this is the first place to look for appropriate lessons and models that can be applied to MDA. Strategic level planning is a long established function of the military services, which routinely conduct strategic level analysis for operational and campaign planning. All branches of the military and most government agencies maintain some form of strategic center for senior officers and analysts to compile and act on strategic level information in this regard. In recent times, the advent of “net-centric” systems that allow strategic planners almost live feed from operational units have increased the utility—and complexity—of these centers considerably.

---

<sup>47</sup> *National Plan to Improve Maritime Domain Awareness*, 4.

From the strictly military perspective, strategic command centers are inherent to all services, and it would seem that such centers would be tailor made for the implementation of MDA. But MDA brings with it several unique challenges that challenge this assumption. Most military command centers are defense specific, focusing on military command systems and operations. Government and law enforcement agencies, while similar in many respects, do not exercise the same procedures.<sup>48</sup> The unique multi-agency nature of MDA requires that any center quantifying strategic MDA must not only focus on strategic maritime issues but also have the ability to link and liaison with participating agencies in both DOD and DHS at a strategic level. The very nature of the global maritime environment requires that this center be integrated cross-government, possessing the ability to gather, analyze, and disseminate data from a wide variety of tremendously diverse sources, including DOD, law enforcement, DHS, Department of State, Department of Transportation, Department of Commerce, private industry, etc. Additionally—and this is a key distinction—it must be recalled that MDA is ultimately about awareness, not the operational direction of forces. A center focused on strategic MDA must act as an enabler for organizations by obtaining this awareness, not a controller for military or law enforcement operations.

A center for strategic MDA must have experience in multi-agency operations and procedures that can transcend the gap between the military, law enforcement, and regulatory agencies that are part of MDA. In the maritime arena, this is possible through expansion of existing infrastructure, specifically developing such a fusion/analysis point at the National Maritime Intelligence Center (NMIC). NMIC was designed as a unique multi-agency approach to general maritime intelligence, housing the Office of Naval Intelligence (ONI), the Coast Guard's Information Coordination Center (ICC), and Marine Corps Intelligence Activity (MCIA). Additionally, NMIC has active liaison and interface with the Drug Enforcement Agency (DEA), CBP, ICE and other DHS agencies with interest in the maritime domain.<sup>49</sup> Through this initial design many of the

---

<sup>48</sup> Gregory Treverton, "Intelligence: Welcome to the U.S. Government," in Loch K. Johnson and James J. Wirtz, *Strategic Intelligence* (Los Angeles: Roxbury Publishing, 2004), 351.

<sup>49</sup> Bill Tarry, "Building the NMIIC," unclassified briefing to OPNAV, Pentagon, October 2004.

communications and liaison problems inherent in a purely military structure were significantly reduced; NMIC has a history of working with other agencies in compiling maritime intelligence. This liaison activity has increased significantly since 9/11 with an increased focus on maritime security and counter-terrorism on the strategic level.

NMIC is particularly suited for strategic MDA in a number of respects. Employing a unique multi-agency approach to conduct worldwide civil-maritime analysis, NMIC increases its emphasis on HLD, standing up a dedicated watch floor with connectivity to various COCOMs and HLS agencies. From the analytical perspective, ONI is the principal source for maritime intelligence on global merchant affairs and a national leader in other non-traditional maritime issues such as counter-narcotics, fishing issues, ocean dumping of radioactive waste, technology transfer, and counter-proliferation.<sup>50</sup> These programs have direct applicability to strategic MDA. Through a long-term, massive compilation of data obtained from a variety of sources (much of which is commercially available), NMIC uses its Global Trader database system to baseline normalcy in the merchant shipping worldwide, enabling it to detect anomalies,<sup>51</sup> perform pattern matching on illicit activity, and alert to high interest profiles.<sup>52</sup> Analysts are employed who possess merchant marine background to provide a civilian perspective on merchant activity, as well as port and customs experts in addition to regular Navy and Coast Guard personnel.

Analysts at NMIC focus on “white” (non-military) shipping, cargo-container movement, and international port activity. In analyzing the entire transshipment process, they have been successful in obtaining information on roughly 40% of all containerized

---

<sup>50</sup> Office of Naval Intelligence, <http://www.fas.org/irp/agency/on intro.htm>. (accessed September 30, 2005)

<sup>51</sup> “Anomalies” in the military context requires some explanation. Most vessels in a naval COP are not tracked continuously unless there is some reason to suspect illicit activity—the track is required to be ‘updated’ over several hours, or, as seen in the MDIZ example, verified with increasing frequency as the vessel approaches the U.S. coastline. This verification is usually done with some form of active or passive sensor. Between verification, however, the vessel’s position is assumed using its last known course and speed. Obviously if the vessel changes course, the estimated position will not be accurate during the next tracking verification, creating an uncertainty or anomaly. This can also be applied in analysis. If, for example, a vessel with a known history of carrying one type of cargo on a set route suddenly changes its manifest or destination, this could be seen as an anomaly worthy of further investigation.

<sup>52</sup> Wendy Kay, NMIC brief to author, Suitland MD, 9 March 2004.

cargo worldwide.<sup>53</sup> Additionally, through a number of international agreements with inter-model shipping agencies, open source data is collected on most of the major ports and maritime transshipment points worldwide. This data is used not only to detect anomalies, but also to address seams between the different modes of transportation from an all-domain viewpoint. NMIC maintains active liaison with Customs efforts in executing the Container Security Initiative (CSI), sharing appropriate data to improve security for containerized cargo.

Prior to 9/11 NMIC was generally recognized as one of the premier centers for strategic maritime intelligence. For purposes of MDA, however, several key elements are missing that are required to meld it into the developing MDA infrastructure as the focal point for strategic MDA. The first is a formal recognition that NMIC should fulfill this role. Today many agencies maintain independent strategic intelligence centers with limited ties to NMIC, effectively stove piping their strategic intelligence<sup>54</sup>. Unlike JHOCs and MIFCs, the inter-agency integration at the strategic level is not nearly as well developed as that employed at local or regional levels, where often cooperation is based on local relationships or a shared operational area. Recognition of NMIC as the strategic center for MDA will require the establishment of formal liaison billets and links to other agencies at the highest level of government. The recent reorganization of the intelligence community and the creation of the Terrorist Threat Integration Center (TTIC) can serve as a model for the new NMIC to follow for MDA.<sup>55</sup>

Second, NMIC must be linked via an active COP or dedicated link to JHOCs, MIFCs, and DOD combatant commanders. This exists to a large extent in its legacy support to Navy and Coast Guard COCOMs via an active watch and operations center

---

<sup>53</sup> Wendy Kay, NMIC brief to author, 9 March 2004.

<sup>54</sup> The most detailed public examination of stove piping and other harmful intelligence practices prior to 9/11 are stated in *The 9/11 Commission Report* (New York: W.W. Norton, 2004), Chapter 11 “Foresight and Hindsight,” particularly sections 11.3-11.4.

<sup>55</sup> The creation of the Director of National Intelligence is one of the most sweeping Intelligence reorganizations since the National Security Act of 1947. See “White House National Intelligence Director Press Briefing,” ([www.whitehouse.gov/news/releases/2004/08/2004082-6.html](http://www.whitehouse.gov/news/releases/2004/08/2004082-6.html)), August 2, 2004, accessed February 26, 2005)

that monitors fleet activity for both Services.<sup>56</sup> This link needs to be strengthened, focusing on direct inter-action with JHOCs, and MIFCs, using multi-agency liaisons to analyze the data flowing from these sources for strategic MDA. Such a COP will allow MDA information to flow unimpeded to the strategic level for analysis, while subsequently allowing information and analysis to flow directly back down the chain.

The new NMIC would have a number of distinct roles and responsibilities in the MDA realm. This includes long term analysis to identify potential enemy trends in the maritime domain, and providing Indication and Warning analysis (I&W) by piecing together indicators that may identify potential terrorist action/attack. This information would be translated into actionable intelligence that can be inputted to the COP for immediate dissemination to the MDA operational and tactical levels and applicable COCOMs and agencies. In addition to its I&W responsibilities, information fusion and integration at NMIC allows for true compilation of maritime data that is vital for strategic planning, including generation of worldwide shipping lists, potential overseas cargo tracking and trends, WMD and counter-proliferation studies, port vulnerability analysis, and other long-term analytical studies that provide critical background for operational planners. As part of the MDA infrastructure, this information would flow freely in a cyclical manner between regional and tactical levels via the COP.

---

<sup>56</sup> Wendy Kay, NMIC brief, 9 March 2004.

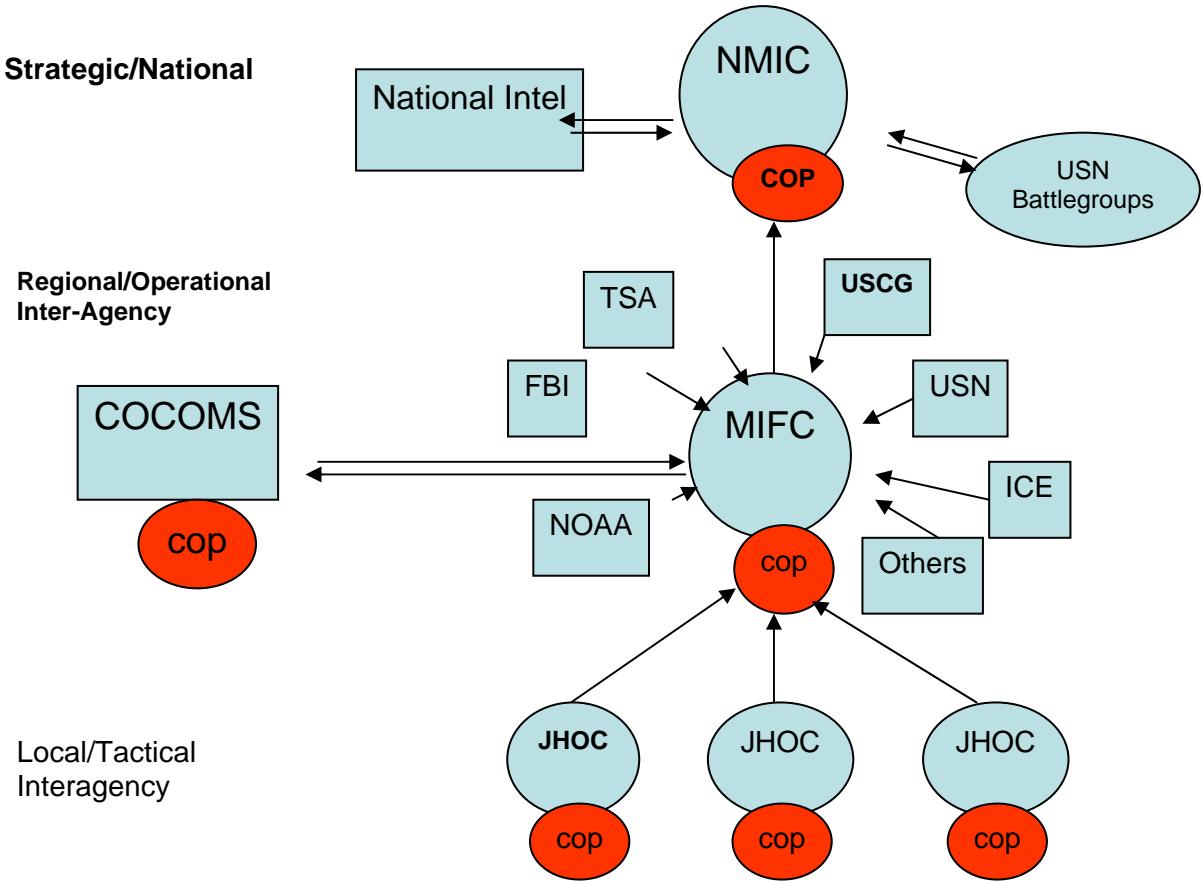


Figure 6. Current Infrastructure Model

Figure 6 illustrates the full Current Infrastructure Model on the Tactical, Regional, and Strategic levels. Note that although there is some degree of hierarchy in these relationships, they are intended to be fully cyclical. Information is shared via the COP between organizations at each level. In other words, there is no senior-subordinate relationship between the groups; information flows freely and is used by respective analysts to focus on their areas of expertise.

Legacy systems at NMIC provide a final key component of strategic MDA that make it truly global in perspective. Through its fleet support, NMIC exercises a link to dedicated overseas elements that can contribute to the strategic picture through robust and active surveillance. For purposes of the MDA model, this can be improved in a number of ways. In the immediate aftermath of 9/11, Customs established a number of overseas positions for shipping agents to perform cargo checks on containers bound for the United States. This program has direct applicability to the cargo analysis element of MDA.

Linking cargo information to NMIC for analytical purposes would be of enormous benefit to strategic MDA.<sup>57</sup> Operationally, deploying Navy battle groups maintain a robust surveillance capability during their transit to operations areas and while on station, providing this information to the Navy's global COP. Possessing organic sensors that can be tasked to look at specific areas or threat, and maintaining active intelligence links, Navy battle groups can act as "deployable MIFCs" vis a vis MDA, providing overseas information that can be extremely valuable to strategic analysis conducted at NMIC. This mobility and the ability to conduct surveillance at various straits and chokepoints can make a key contribution to the MDA COP, especially if intelligence indicates potential "hot spots" of maritime threat activity.

No discussion of global MDA would be complete without consideration of National Assets that can be fused into the strategic picture maintained at NMIC. The United States maintains two distinct forms of sensors that have particular applicability to MDA: a robust satellite capability maintained by the National Security Agency (NSA) and National Reconnaissance Office (NRO), and the Integrated Underwater Surveillance System (IUSS).<sup>58</sup> Developed during the Cold War, these systems offer superior capability for ocean surveillance, enabling in-depth analysis and I&W by NMIC. While specific capability is classified, both NSA and NRO have become full partners in the MDA effort, and are currently studying methods by which these systems can be re-tasked from examining a strictly military/Cold War threat to a broader application for use in MDA. This is possible through linkage with NMIC, which already has a long established history in liaison with these commands and background in analyzing data provided from national assets.<sup>59</sup>

---

<sup>57</sup> Cargo and container analysis is actually far more complex than simple inspection; at present, CBP uses a number of computer programs in conjunction with inspectors to check for anomalies much in the same way vessel tracking systems are employed. These programs are part of the broader Container Security Initiative (CSI). See [www.cbp.gov/xp/border\\_security/international\\_activities/csi](http://www.cbp.gov/xp/border_security/international_activities/csi). (accessed September 25, 2005).

<sup>58</sup> The capabilities of these systems are highly classified and beyond the scope of this thesis. For an unclassified overview, see [www.fas.org/irp/program/collect/iuss.htm](http://www.fas.org/irp/program/collect/iuss.htm). (accessed March 19, 2005)

<sup>59</sup> Wendy Kay, NMIC brief, 9 March 2004.

An expansion of NMIC to focus on strategic integration would place the facility as the lead strategic component of MDA that has uses in the national arena in established areas of counter-terrorism and homeland defense. This inter-governmental integration also creates a centralized location for maritime intelligence that can be used by other commands and agencies (for example, the National Counter Terrorism Center and NORTHCOM) to meet their maritime intelligence requirements for GWOT and Homeland Defense. By enhancing the established facility with inter-agency liaison positions and creating a global COP, NMIC can effectively bridge the gap between homeland security, Department of Defense, and National Intelligence agencies with a vested interest in both HLS and HLD.

#### **D. SUMMARY OF THE CURRENT INFRASTRUCTURE MODEL**

MDA is about information, and as we enter the high tech world of the 21<sup>st</sup> century it is apparent that information is available in abundance. At no time in history has so much information been available to operational commanders, but conversely, the huge amount of data that must be considered in the maritime domain often threatens to overwhelm traditional military and civilian analysts. This is the great paradox of our time. As the 9/11 report aptly stated, to be truly effective we must not focus on collection, but rather devise an effective method to sort the wheat from the chaff, to bring together these vast sources of information in one coherent picture to determine what is applicable to homeland security and homeland defense.<sup>60</sup>

The Current Infrastructure Model capitalizes on infrastructure and expertise traditional organizations had prior to 9/11 fused with new structures put in place to deal with the new asymmetric threat. As we have seen, much of the work has already been accomplished, either through the creation of new command structures (JHOCs and MIFCs) or by intelligence organizations re-focusing their efforts on maritime homeland security (NMIC). By refocusing the “best of breed” multi-agency group in each level of warfare—tactical, regional/operational and strategic—toward the common goal of MDA, by linking what we already have through shared situational awareness and by dedicated

---

<sup>60</sup> *The 9/11 Commission Report*, 399-428.

analytical effort, we can achieve MDA at a minimum of cost and maximum efficiency. By making this an inter-agency effort using established Coast Guard (DHS) and Navy (DOD) components, the legal barriers currently in place regarding information exchange can be addressed.<sup>61</sup>

Implementing MDA by employing the Current Infrastructure model of linking JHOCs, MIFCs, and NMIC offers a number of unique advantages:

- Employs a natural multi-agency approach by fusing intelligence at the three respective levels (tactical/operational/strategic)
- Approaches MDA as an information system to enable current operations, not a system designed to drive operations
- Does not require a command element; rather, emphasizes that information is available for all to use and is therefore a force multiplier vice a driver.
- Employs current infrastructure with minor modifications making it cost effective and easier to implement.

---

<sup>61</sup> See Appendix 2.

#### **IV. ALTERNATIVE MDA MODELS**

While MDA is not new, it is an evolving concept and far reaching in its scope and vision. The idea of a unifying system of fused multi-agency information is entirely new to both DOD and DHS, and as such has been subject to a great deal of debate. This is especially true regarding the final form that MDA will take upon implementation. MDA cannot just “happen” on its own; clearly there must some form of construct and oversight to ensure its success. But the final forms this can take vary considerably. On one end of the spectrum, the Current Infrastructure model describes a construct that shares information with a minimum degree of command and control, focusing on the linkage of established infrastructure toward the common goal of MDA. On the other, arguments have been made that given the diverse and multi-agency nature of MDA, a more rigid command and control structure is required.<sup>62</sup> This could take the form of establishing a formal command to focus specifically on MDA, controlling various operational assets to achieve multi-agency awareness. The idea of creating new commands to specialize in a particular region or operational area of expertise is not new; DOD has been using the Joint Task Force (JTF) concept in this regard since the 1980s. But JTFs are intended—in theory—to be narrowly focused and above all temporary. The command models expand on this concept to argue for a permanent state, one strategic entity that effectively controls all elements of MDA.

Two models figured prominently in the command debate. Since MDA is a relatively new, multi-agency concept, these models focus on a structure that would bring various agencies together under one form of new command that would ensure the implementation and continued exercise of MDA. The first, the creation of a “Maritime NORAD” calls for a structure similar to that used to protect the air approaches to the United States, while the second, a Joint Inter-Agency Task Force (JIATF) relies on a joint model that became popular in the 1980s. Interestingly, both models are based heavily on historical successes in other domains. Created in 1958, NORAD is a well designed and

---

<sup>62</sup> Donna Miles, “Planning Group Weighs Value of ‘Maritime NORAD,’” *Armed Forces Info Service, Defense Link News*, 17 May 2005.

coordinated air defense entity whose construct and procedures, advocates argue, could easily be adapted to the maritime domain. The JIATF model is borrowed heavily from the multi-agency counter-narcotics command created in 1989 to focus on DOD involvement in countering drug trafficking. Proponents of this model argue that a “JIATF MDA” could, in theory, expand efforts from counter-narcotics to all activities in the maritime domain. The strengths—and weaknesses—of these models will now be examined in turn.

#### A. MARITIME NORAD

The North American Aerospace Defense Command (NORAD) is seen by many—including the former Chief of Naval Operations—as an effective model for maritime defense.<sup>63</sup> There are good reasons for this. Formed in 1958 as a multi-national organization to defend North American airspace, NORAD was the first command to deal specifically with defense in one strategic domain, utilizing a vast array of extremely technical assets to perform its mission. NORAD has vast experience in fusing highly technical means, national assets, and other information sources into one comprehensive surveillance system that has been extremely effective in monitoring and responding to potential air threats to the United States. NORAD is unique in its mission and extensive capability, effectively coordinating strategic and tactical operations in one domain. Its ability to effectively monitor one domain and respond quickly to a perceived threat either globally or regionally make NORAD a very attractive command and control construct for a similar MDA organization. Moreover, NORAD is both bi-national and multi-agency, elements required in any final form of MDA. Given the similarities between the capabilities of NORAD and the requirements of MDA, it would seem that replicating this model in the maritime arena is a logical choice to implement MDA.

While it is true that NORAD’s success in the air domain make it an attractive alternate model for MDA, there are several immediate problems adapting its structure to the maritime domain. NORAD is a purely reactive command, intended as a defensive model. Due to its global nature and the need to seek out all information relevant to the

---

<sup>63</sup> Robert Ackerman, “Pace of Change Accelerates for U.S. Navy,” *Signal Magazine*, December 2004.

maritime domain, MDA is not a defensive organization, but rather a concept focused on aggressive collection and analysis. Vessel tracking is a key component of MDA, but as we have seen MDA is ultimately an information system that attempts to fuse all of the elements of interest that touch the maritime domain, such as cargo anomaly detection, tracking of suspect personnel, determining vessel links to terrorism, and a myriad of other intelligence or informational components. The NORAD model does not emphasize long term analysis of these factors per se, rather focusing on the detection, tracking, and interception of established threats. Much of the information that is so crucial to the success of MDA is non-traditional, non-military, and multi-agency in nature, and as such is generally not available to traditional military commands. The requirement to correlate this wide ranging type of information for an effective tactical and strategic picture is far more detailed than that addressed by the NORAD model.

The global nature of MDA also presents difficulty when considering the NORAD construct. NORAD was designed to focus strictly on the North American area of responsibility (AOR), and as such is partnered with Canada in a bi-national effort. The implementation of a “maritime NORAD” also implies this North American centric viewpoint, which will present diplomatic problems in partnering with other nations, notably Mexico which has repeatedly indicated it will not participate in a defensive type organization.<sup>64</sup> A distinct militarization of MDA as a NORAD has the potential to create similar reactions from other international partners that are crucial to effective MDA execution.

Arguably these difficulties can be overcome. No one is saying the actual command and control structure used by NORAD should be moved directly into the maritime domain. The idea of a maritime NORAD is largely conceptual, but as an actual command structure would be in place to conduct maritime surveillance operations, it is logical to assume that this role would be assigned to Northern Command (NORTHCOM), the DOD command charted with coordinating homeland defense in the

---

<sup>64</sup> Lawrence Spinetta, “Expanding NORAD: A Strategy to Engage Mexico.” *Air Power International*, 24 June 2004. [www.airpower.maxwell.af.mil](http://www.airpower.maxwell.af.mil). (accessed April 30, 2005).

continental United States.<sup>65</sup> DOD created NORTHCOM to coordinate Pentagon homeland defense efforts and allocate military support to civil authorities.<sup>66</sup> In this role, if there were to be a formal “Maritime NORAD,” it would seem that NORTHCOM would be the logical place for such a command to be created.

As DOD’s primary HLD command, NORTHCOM’s area of responsibility includes defense of the continental United States (including Alaska, Puerto Rico, and the USVI) and the Atlantic and Pacific Ocean within approximately 500 miles of the United States.<sup>67</sup> Physically co-located with NORAD, NORTHCOM’s over 1200 personnel are drawn from all Services in DOD and include representatives from the Coast Guard and other multi-agency liaisons. Representing one of the largest military reorganizations since the Second World War, NORTHCOM’s responsibilities include not only homeland defense, but also focus on Military Assistance to Civil Authority (MACA) for consequence management. This is a tremendous degree of responsibility and requires considerable diversity in operational expertise.

NORTHCOM’s mission focus makes its use as a maritime NORAD problematic. As a DOD Combatant Commander (COCOM), NORTHCOM’s primary responsibility is HLD, not HLS. In the inter-agency construct, this is a far bigger legal and policy issue than one might imagine. As previously discussed, HLS is primarily a law enforcement mission involving non-DOD agencies.<sup>68</sup> While it is true that NORTHCOM has established liaison with many civilian agencies for HLS and MACV operations, the scope of MDA would require a huge expansion of these relationships. Moreover, unlike the Current Infrastructure model, the NORAD construct implies command, not cooperation. Many of the agencies that operate under the DHS umbrella that are potential

---

<sup>65</sup> Note that NORTHCOM is only one proposal as to the final form of a maritime NORAD. The idea that NORTHCOM should take the role of Maritime NORAD, however, has been proposed a number of times within DOD. While there are other candidates, the author concedes that this is the logical choice for such a command given proposed structure of a maritime NORAD and the fact that NORTHCOM is currently in place and located with the current NORAD. If we were to have a NORAD-like command, NORTHCOM is the logical choice.

<sup>66</sup> Jason Sherman, “Domain Defense,” *Sea Power*, [http://www.navyleague.org/sea\\_power](http://www.navyleague.org/sea_power), May 2004, (accessed February 26, 2005).

<sup>67</sup> NORTHCOM Strategic Vision, 4.

<sup>68</sup> See Appendix 1.

users/contributors to MDA would have a difficult time operating under a military command structure that is completely foreign, in addition to a host of legal issues that could arise from such an arrangement.<sup>69</sup> Finally, NORTHCOM's area of responsibility both geographically and operationally is also extremely large. Taking on the considerable responsibility of also acting as a maritime NORAD would require considerable refocus, including a massive influx of personnel and equipment to tailor the command to the new maritime mission in both its HLD role and to meet the strategic world-wide information gathering requirements of MDA.

## B. JIATF

A Joint Inter-Agency Task Force (JIATF) model differs from the maritime NORAD construct in several key areas. The JIATF construct was designed for and has been used successfully in the counter-narcotics arena since the early 1990s. Although a military command, JIATF is far more specialized than standard JTFs and intended from its onset to be a multi-agency organization. JIATF is extremely focused on one particular mission area, fusing various intelligence and operational components from both DOD and law enforcement toward that mission. The original intent of JIATF was to use the DOD intelligence to detect and monitor air and maritime narco-trafficking, passing this information to appropriate law enforcement activity for action once the threat had been properly localized. The model used for MDA is based on the current counter-drug organization, JIATF SOUTH.

JIATF SOUTH's official mission statement is to "conduct counter illicit trafficking operations, intelligence fusion and multi-sensor correlation to detect, monitor, and handoff suspected illicit trafficking targets; promotes security cooperation and coordinates country team and partner nation initiatives in order to defeat the flow of illicit

---

<sup>69</sup> See Appendix 2.

traffic.”<sup>70</sup> Officially created by Presidential Decision Directive 14 in 1989, the JIATF construct was in direct response to President Reagan’s decision that drug smuggling represented a clear and present danger to the United States and as such was subject to action by DOD vice traditional law enforcement.<sup>71</sup> As a DOD entity, JIATF’s mission was limited strictly to detection and monitoring of suspected drug trafficking. Actual seizure was conducted by units under the tactical control of the Coast Guard. This legal nicety allowed for the use of considerable DOD surveillance assets while avoiding actual combat under DOD per se. As such, JIATF proved to be the first (and arguably most successful) merger of military and law enforcement capability to meet a common threat.

The unique advantage of the JIATF model is its interagency construct designed to fuse intelligence and operations. Representatives from the Department of Defense, Department of Homeland Security (Coast Guard, formally under DOT), and Department of the Treasury (Customs) work side by side with representatives from the DEA, FBI, DIA, and NCIS. In addition, JIATF utilizes effective international liaison with Great Britain, France, Canada and the Netherlands who provide ships, aircraft and liaison officers. A recent development is the inclusion of liaison officers from Argentina, Colombia, Ecuador, Peru, and Venezuela, all of which have a vested interest in stopping the maritime drug trade.<sup>72</sup>

Given its unique multi-agency intelligence and operational construct, as well as its noted success in fusing intelligence that can be used by all participants, it would seem that the JIATF construct would be perfect for an MDA command and control construct. Culturally, the formation of JTFs to deal with specific military threats is an established military procedure, and there is no questioning the success of JIATF in the counter-

---

<sup>70</sup> [www.jiatf.southcom.mil](http://www.jiatf.southcom.mil). (accessed January 8, 2005) Note that “JIATF SOUTH” is a relatively new command designation. Originally designated JTF 4, the JIATF mission evolved into two separate commands based on geographic areas of responsibility; JIATF EAST covered drug traffic in the Atlantic/Caribbean, while JIATF WEST focused on the Pacific. In 2002 a reorganization occurred due to shifting trafficking emphasis; the newly designated JIATF SOUTH focused on the Caribbean/Eastern Pacific, while JIATF WEST focused on the western Pacific. For purposes of this discussion, the lessons learned/operational description will be taken from historical efforts in the Caribbean as this is the highest area of trafficking and JIATF operations.

<sup>71</sup> [www.globalsecurity.org/military/agency/dod/jiif.htm](http://www.globalsecurity.org/military/agency/dod/jiif.htm). (accessed January 8, 2005).

<sup>72</sup> [www.globalsecurity.org](http://www.globalsecurity.org). (accessed January 8, 2005).

narcotics mission. These factors were subject to considerable debate in the immediate aftermath of 9/11 and a large war gaming effort gave considerable weight to the argument to form a new JIATF focused purely on MDA.

The JIATF model, however, has two primary weaknesses as a construct for MDA. The degree of effort and scope required to achieve MDA, and JIATF's relationship to operational forces are challenges to the JIATF model. As we have seen, MDA is an all-encompassing global information system of considerable scope, requiring a strategic viewpoint vice operational. It must be recalled that JIATF was formed to perform a limited mission against a very specific threat in a relatively limited operational area. The specialists at JIATF use surveillance, intelligence, and analysis against maritime smuggling, which utilizes a very specific skill set. While JIATF is very good at detecting and tracking potential smugglers in its area of responsibility (in JIATF SOUTH's case, the Caribbean), an expansion to cover all events in the maritime domain is another matter. Like a maritime NORAD, such an expansion would require a massive influx of personnel whose expertise covers the full gamut of MDA.

JIATF's employment of operational assets is problematic when translating its construct to MDA. Counter-narcotics is focused on detecting and tracking a known "enemy" threat—MDA, as an information system, is far less active or adversarial. In the present state, JIATF actively employs military assets to search for, track, and intercept smugglers. To perform this mission, assets (ships and aircraft) are "loaned" to JIATF from the respective services for patrol and intercept, much like any other COCOM dealing with a specific threat. While actual numbers are classified, the forces assigned are relatively small as they are scaled to the operational area. This issue of mission scale is significant when considering potential operational forces assigned to MDA. While conducting surveillance and intercepting drug smugglers requires relatively few assets in the grand scheme of U.S. military force, actively dedicating assets to conduct global MDA using a JIATF construct would not. Dedicating even a moderate number of assets

to MDA on a continuous basis would have a serious impact on overseas operations.<sup>73</sup> MDA's global nature of MDA—awareness in every theatre, especially closing the coastline of the United States—also brings about potential conflicts with other established organizations as other military commands whose area of responsibility come into conflict with a JIATF MDA. In theory, if MDA is in fact a state of situational awareness/information system, all maritime assets should be contributing to the information system. If a JIATF is dedicated to MDA, would it take control of and direct assets that are, in fact, conducting essentially the same mission for another commander?<sup>74</sup> This potential conflict of interest violates the premise of unity of command, and represents tremendous potential for mismanagement of assets, conflicts, and turf battles.

Finally, one must consider the tactical and legal implications of employing military assets in this manner. In the early days of JIATF, a number of military assets were used to actively patrol various areas in the Caribbean in the effort to detect smugglers. Tactically, this proved to be a misuse of assets as smugglers simply diverted around the established locations.<sup>75</sup> Finally, the counter-narcotics JIATFs were designated (and limited) by specific legal authority to target a threat to national security. MDA, as an information system, enjoys no such authority. Employing DOD assets to actively search and potentially board targets of interest without specific intelligence or established Title 14 authority is a difficult legal challenge that must be addressed by legislation if it is to be effective.

---

<sup>73</sup> Naval vessels go through a rigorous training cycle prior to overseas deployment, sometime in the order of 6 months of “workup” exercises, small local strike group exercises. This is rigorously controlled by fleet commanders. If a ship were taken out of this training cycle for patrol duty, it would take much longer to enable it to be fully trained for overseas duty. Additionally, as there are a limited number of ships for overseas assignment, another ship would have to be rotated into the cycle early, creating either a training shortfall in that ship’s preparation or a delay in scheduled maintenance. This has a considerable “snowball” effect on the overall system, creating significant gaps fleet wide. Author’s operational experience.

<sup>74</sup> For example, if a Coast Guard cutter is performing an operational mission off the U.S. coastline under the operational control of the Coast Guard (and, in theory, conducting MDA in the process), would a JIATF suddenly “take control” of that asset for another MDA related mission? This has the overall effect of operational assets working for “two bosses,” a very difficult and confusing operational problem.

<sup>75</sup> Author’s operational experience. The “ship in a box” tactic, while effective in detecting strictly military threats to a strike group, is poorly adapted to law enforcement or surveillance operations. As JIATF operations matured through experience, it was determined that active use of intelligence combined with the use of military assets was far more effective in counter-narcotics operations than simply assigning ships to patrol certain ocean areas.

Both the JIATF and the NORAD concepts differ from the Current Infrastructure Model in that proponents see the need for some directing force—a command—to ensure effective MDA. The crux of the MDA command models is twofold: that information must be managed by a centralized authority to be effective, and that operational assets must be dedicated solely to the MDA mission. These premises ignore the very nature of MDA. In terms of information management, the global nature of MDA and the diversity of knowledge and expertise required to make it effective is a direct counter to the centralization argument. Collating this vast amount of information in one place would not only swiftly overwhelm a single command entity, but also significantly diffuse the tactical and operational levels that actually use MDA in their individual operating areas. In terms of operational direction of assets, ultimately MDA is not about directing ships and planes to chase down every potential unknown contact on a continuous basis, it's about the effective use of sensors and information flow to provide operational commanders the intelligence to direct those assets.

The Current Infrastructure Model addresses both issues by delegating MDA to appropriate levels of authority while focusing on a shared information network. Current infrastructure argues that by its very nature MDA is best managed at the three respective levels of warfare—tactical, regional, and strategic—for information relative to the warfare area and using MDA as a force multiplier for operational units at those levels. Current infrastructure does not require the dedication of operational assets per se to the MDA mission, as it is assumed that MDA will become a mission subset of all fleet operations and thus contribute naturally to an overall shared COP.

THIS PAGE INTENTIONALLY LEFT BLANK

## V. SUMMARY

The vulnerability of the maritime domain is one of the most serious security challenges facing this nation. The United States' reliance on the sea has not changed with the onset of the Global War on Terror. If anything, this reliance has been increased by the demands of globalization and the increased requirement to rapidly deploy military force worldwide. The tremendous diversity and complexity of the maritime domain and the potentially catastrophic effects of an enemy attack make its protection a top national priority. Key to protecting the maritime domain is obtaining information vital for planning, multi-agency cooperation, and operational response. That is Maritime Domain Awareness' role.

MDA is extremely ambitious in scope, vision, and stated objectives. As one of the largest security programs undertaken by the U.S. government, effective MDA will require considerable alignment among the 16 government agencies responsible for its implementation. Much has been accomplished in establishing policies and procedures for improving maritime security, but for MDA to be completely implemented, a new organizational structure will be required that considers execution on a national, regional, and tactical level. The National Plan for MDA is the first step in achieving this goal, but it is only the beginning. The details of how this plan will be implemented remain to be seen. When examining our current capabilities, the use of current infrastructure will be the most efficient means to achieve this implementation.

While the MDA program grew out of the vast governmental reorganization following 9/11, the concept itself is not new. As part of core maritime law enforcement and military operations, the Coast Guard and Navy have always conducted some form of MDA geared toward their respective mission areas. As such, much of the infrastructure, and procedures that were used prior to 9/11 are still in place, and can be effectively modified to meet the increased demands of a total maritime awareness system. This is possible by considering infrastructure vis a vis the new requirements of MDA. On the tactical level, the JHOC initiative shows great promise by fusing Coast Guard and Navy port operations with the myriad of regulatory and law enforcement agencies active in

ports, creating one common information system that can be used at a centralized location by all parties. Regionally, the newly created MIFCs can link with JHOCs to provide analysis and disseminate critical information up the chain to strategic centers and back down to tactical users. As an experienced national intelligence center, the NMIC can act in the strategic role fusing information from the tactical and regional levels, while providing a broader picture for long-term planning and global operations. Through a dedicated virtual link, the combination of this infrastructure under the over-arching goal of MDA can be an effective and easily implemented solution to the post 9/11 maritime security challenge.

## **APPENDIX 1: HOMELAND SECURITY AND HOMELAND DEFENSE**

### **A. BACKGROUND: WHY TWO MISSIONS?**

While historically the military has always had a role in defending the homeland, these actions have generated deeply rooted concerns about the use of military force on U.S. soil. The Posse Comitatus Act restricting domestic use of the military was written to reflect this viewpoint. Although the military has been used in active defense during wartime, this has been against a direct and specific military threat (such as the U-boat attacks during the Second World War, and the formation of NORAD to defend against Soviet missile attack). More recently military actions have moved beyond strictly conventional roles, supplementing certain “lower intensity” law enforcement style operations, such as providing surveillance and intercept capability in the Drug War and countering illegal immigration.<sup>76</sup> Regardless of the success or increasing frequency of these operations, the military has moved cautiously. The encroachment of the military into traditional law enforcement missions has moved slowly—if at all—and under extreme scrutiny by lawmakers and the public.

This mindset changed after the 9/11 attacks and the subsequent launch of the “Global War on Terror” (GWOT). While it is true that Posse Comitatus remained unchanged, the direct attack on the United States and subsequent GWOT placed the military on a war footing. Despite its offensive, overseas nature, the overriding priority in GWOT is protection of the homeland, a mission assigned top priority by the military. Yet determining how the military is to accomplish this mission has proved challenging. In the immediate aftermath of the mobilization following 9/11, no additional threat materialized in the homeland, leaving the DOD’s contributions to homeland defense unclear. It was immediately apparent that the nature of this new war presented several unique challenges. Although terrorists are armed enemies, their ability to hide and operate domestically placed many of their acts solidly in the realm of law enforcement,

---

<sup>76</sup> Recent expansion into LE operations, notably in the “Drug War” were enacted during the Reagan administration which broadly defined national security threats that were valid targets for the military..

which is, admittedly, far better trained and equipped than the military for lengthy investigation and apprehension. But unlike those who have committed previous terrorist acts on U.S. soil, Al Qaida are outfitted and trained outside of U.S. borders specifically to conduct “warfare” against the United States, arguably making them combatants. Clearly, both domestic law enforcement and the military have parts to play in this new war. “War winning” is not confined to the military alone.

The recognition of this new element in warfare and the differences between law enforcement and military action resulted in the creation of the respective missions of Homeland Security and Homeland Defense. In their strategies DHS and DoD define these missions as:

Homeland security (HLS) is. . . “a concerted national effort to prevent terrorist attacks within the United States, reduce America’s vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. The Department of Homeland Security (DHS) is the lead federal agency for homeland security.<sup>77</sup>

conversely,

Homeland defense (HLD is. . .the protection of U.S. sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression. The Department of Defense (DOD) is responsible for homeland defense<sup>78</sup>

Further quantifying these definitions, it would be fair to say that HLS is confined to the realm of law enforcement (with possible DoD assistance), while HLD is a DoD mission employing military assets.

The intent in creating separate mission areas is twofold. In defining separate missions we have neatly aligned our cultural tradition of separation of civil and military authorities, while assigning responsibility for counter-terrorism where appropriate. This places the agencies in their respective “boxes” where they can apply their individual capabilities and expertise in the most efficient manner. Additionally, one must consider

---

<sup>77</sup> *National Strategy for Homeland Security*, 2.

<sup>78</sup> *Strategy for Homeland Defense and Civil Support*, 10.

that separation of missions into HLS and HLD allow for considerable law enforcement assets (and perhaps more importantly, expertise) to be brought to bear on a security problem where a strict application of military force is not appropriate (and may be, in fact, counter-productive).

Although defined, there has been much speculation as to what exactly constitutes an HLS and HLD event and, more importantly, when the “line” is crossed. In making this determination, a number of guidelines are employed:

1. Almost all security threats begin in the HLS realm. This is due to the fact that most events are usually nebulous or uncertain at the outset, requiring some degree of investigation. There are two exceptions to this:

a. The threat is a known WMD. In this particular case, it is usual to define the event as HLD and military action is taken.

b. The threat is airborne. To date, DHS has no air intercept capability, so these threats are classified as HLD as a responsibility of NORAD.

2. Although an event may be classified as HLS or HLD, this does not mean that forces from DHS or DoD act in a vacuum. In the maritime arena, a number of Memorandum of Agreements (MOAs) exist between Coast Guard and Navy to allow for “chop” (assignment) of forces to each respective Service if the need arises. If, for example, the Coast Guard is attempting to locate a suspect vessel under HLS and requires assistance, it can request ships and aircraft from the Navy to assist in that search (the assets temporarily becoming part of the Coast Guard.) Similarly, in an HLD event the Navy may require the unique boarding capability possessed by the Coast Guard, and can request assets to perform that mission under Navy control for HLD.

3. DHS and DoD share information at the highest levels during developing HLS/HLD events. If the event shows signs of escalating to HLD (i.e., presence of WMD

or clear terrorist threat the HLS cannot meet), the decision to escalate to HLD is made by the Secretaries of Homeland Security and Defense in consultation with the President.

It should be noted that as an information system MDA is an enabler for both HLS and HLD.

## **APPENDIX 2: MDA LEGAL BRIEF**

MDA represents unprecedented cooperation between government agencies and as such is subject to a number of legal issues and concerns, particularly regarding the use of DHS and DoD assets and personnel operating together in information gathering and law enforcement. MDA planning is subject to extensive legal review by both DHS and DoD to ensure the spirit and letter of the law are followed in its execution. It is important in examining MDA initiatives to be cognizant of the pertinent laws that apply in this review.

**Title Authority:** Forces participating in MDA operate under three specific government titles:

a. Title 10: Title 10 applies to issues of authority and command and control for the Department of Defense. While operating under Title 10, the military works directly for the Commander in Chief and cannot participate in domestic law enforcement.

b. Title 14: Title 14 applies to the Coast Guard and designates that Service as a maritime law enforcement agency. It is important to note that the Coast Guard can also operate under Title 10 for military operations.

c. Title 32: Title 32 applies to the National Guard. While operating under Title 32 the National Guard works directly for the Governor (or Adjutant General) of its assigned state and may be used in traditional law enforcement.<sup>79</sup>

**Posse Comitatus:** Drafted in 1878 to limit the use of the Army in the reconstructionist South, Posse Comitatus (PC) was designed to remove the Army from domestic law enforcement and enforcement of politically volatile Reconstruction Era policies.<sup>80</sup> Since 1878 the underlying principles of Posse Comitatus have expanded to include all Services operating under DOD. While this act is largely misunderstood (among other common misperceptions, many feel it is a constitutional mandate vice

---

<sup>79</sup> Alan D. Preisser, “Understanding Authorities in National Special Security Events” in *Joint Center for Lessons Learned Bulletin*, (Suffolk VA: Joint Warfighting Center, September/December 2002), 1.

<sup>80</sup> For excellent background, see Major Craig Trilbecock, “The Myth of Posse Comitatus,” *Journal of Homeland Security* (Oct. 2000).

statutory law), its fundamental premise continues to be generally reflective of the attitudes of the vast majority of U.S. citizens.

Posse Comitatus means that Title 10 forces cannot be used in active law enforcement (interpreted as actions that would normally require a warrant, such as search and seizure). The courts have held, however, that Title 10 forces can be used in “passive” law enforcement, such as planning and preparation of law enforcement activities to assist the local and federal law enforcement agencies.<sup>81</sup> Additionally, PC does not apply when the President or Congress expressly authorize the use of the military to execute the law. This includes giving the Coast Guard civilian law enforcement authority, calling out the military in times of insurrection and domestic violence (under the Insurrection Act), and enacting general legislation authorizing the armed forces to share information and equipment with civilian law enforcement agencies (10 USC 371-382).<sup>82</sup>

Intelligence Support: U.S. Intelligence activities are subject to Executive Order 12333. EO 12333 was written as a result of intelligence abuses during the latter days of the Vietnam War protest movement, when DoD personnel were used to infiltrate and collect intelligence on dissidents. EO 12333 prescribes specific guidelines for intelligence collection for all government agencies. As related to MDA and the use of DoD/CIA intelligence sharing, the EO 12333 specifically states that Agencies with the Intelligence Community are authorized to:

- (a) Cooperate with appropriate law enforcement agencies for the purpose of protecting the employees, information, property and facilities of any agency within the Intelligence Community;
- (b) Unless otherwise precluded by law or this Order, participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities;

---

<sup>81</sup> Preisser, 2.

<sup>82</sup> Jennifer Elsea, “The Posse Comitatus Act and Related Matters: A Sketch,” *CRS Report for Congress* (Washington D.C.: Congressional Research Service, 6 June 2005), 2.

- (c) Provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency, or, when lives are endangered, to support local law enforcement agencies. Provision of assistance by expert personnel shall be approved in each case by the General Counsel of the providing agency; and
- (d) Render any other assistance and cooperation to law enforcement authorities not precluded by applicable law.<sup>83</sup>

As a general rule, raw data collected by DoD (primarily information that is publicly available) on U.S. persons may be shared with law enforcement but analyzed data may not. DoD may not engage in electronic or physical surveillance of U.S. citizens within the United States without permission from a FISA court.

---

<sup>83</sup> EO 12333, [www.fas.org](http://www.fas.org). (accessed October 1, 2005).

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF REFERENCES

### Theses/Unpublished papers:

Breor, Scott. *Maintain Course and Speed: Command and Control for Maritime Homeland Security and Homeland Defense*. Master's Thesis, Naval Postgraduate School. Monterey, June 2004.

McGrath, James P. "Maritime Homeland Defense Command and Control: What is the Right Arrangement?" paper presented to Joint Military Operations Department, Naval War College, Feb 2002.

Napolitano, Michael K. "Applying Sound Joint Doctrine to Ensure Maritime Homeland Security," paper presented to Joint Military Operations Department, Naval War College, May 2003.

Stevens, Mark. "*As Is*" *National Maritime Domain Protection System*. Monterey: Maritime Domain Protection Research Group, November 2004.

### Strategies:

*Concept of Operations: Maritime Domain Awareness*. Draft 1.29. Washington D.C: U.S. Coast Guard, November 2004.

*Defense Science Board 2003 Summer Study on DOD Roles and Missions in Homeland Security (Vol 1)*. Washington D.C: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2003.

*Maritime Strategy for Homeland Security*. Washington D.C: U.S. Coast Guard, July 2002.

*National Plan to Improve Maritime Domain Awareness*. First Coordination Draft. Washington, D.C.: U.S. Coast Guard, March 2005.

*National Plan to Improve Maritime Domain Awareness*. Pre-Decisional Working Draft. Washington, D.C.: U.S. Coast Guard, April 2005.

*National Maritime Security Response Plan*. Coordination Draft, March 2005.

*National Security Presidential Directive NSPD-41/Homeland Security Presidential Directive HSPD-13*. Washington D. C.: The White House, December 2004.

*National Strategy for Homeland Security.* Washington D.C: Office of Homeland Security, July 2002.

*Navy's 3/I Strategy.* Draft working papers. Washington D.C: OPNAV N512, December 2004.

*Strategy for Homeland Defense and Civil Support.* Washington D.C: Department of Defense, Final Coordination Draft, January 2005.

*The National Strategy for Maritime Security.* Coordination Draft, NSMS writing team, draft working paper, Feb 2005.

*The National Defense Strategy of the United States of America.* Washington D.C.: Department of Defense, March 2005.

Briefings:

“Fusion and MDA Systems.” Office of Naval Research unclassified briefing to Assistant Secretary of the Navy (Research and Development), Pentagon, 31 March 2005.

“JHOC Working Group/Briefing to the Maritime Security Integration Group.” Unclassified briefing, Pentagon, 22 June 2005.

“Maritime Intelligence Fusion Center Capabilities and Operations.” Unclassified briefing to author, Alameda CA, December 2004.

“NAVNORTHFLEETWEST & CGDEFORWEST Maritime Homeland Defense/Homeland Security.” Unclassified briefing to Honorable Paul McHale, Alameda CA, 14 December 2004.

“National Intelligence Director Press Briefing.”  
<http://www.whitehouse.gov/news/releases/2004/08/20040802-6.html>. (accessed February 26, 2005).

“Pacific Area Capabilities and Interoperability for Homeland Security/Homeland Defense.” Unclassified briefing to Honorable Paul McHale, Alameda CA, 14 December 2004.

“Technology Working Group, MDA.” Unclassified Briefing, Coast Guard Innovation Expo, San Diego CA, 2 May 2005.

Goward, Dana. “Joint Harbor Operations Center.” Unclassified briefing to Maritime Security Integration Group, Pentagon, February 28, 2005.

Kay, Wendy. "National Maritime Intelligence Center Capabilities." Unclassified briefing to OPNAV N5jw, Suitland MD, March 2005.

Prevost, Larry. "MIFC LANT." Unclassified briefing to author/OPNAC, Dam Neck VA, 7 June 2005.

Tarry, William. "Intelligence Support to Maritime HLS/HLD." Unclassified briefing to Maritime Security Integration Group, Pentagon, February 2005.

Tarry, William. "Building the NMIIC." Unclassified briefing to OPNAV N3/N5, Pentagon, October 2004.

Interviews/Statements:

High, Jeffrey. Interview by R. B. Watts, 25 March 2005. Transcript. MDA Directorate, USCG Headquarters, Washington D.C.

Nimmich, Joe Rear Admiral. Interview by R. B. Watts, 25 March 2005. Transcript. MDA Directorate, USCG Headquarters, Washington D.C.

Statement by General Ralph Eberhart, USAF, Commander of North American Aerospace Defense Command and States Northern Command, Before the Senate Armed Services Committee, March 25, 2004.

Statement by Mr. Jeffrey High, Director, Maritime Domain Awareness, Before the Subcommittee on Coast Guard and Marine Transportation Committee on Transportation and Infrastructure, United States House of Representatives, October 2004.

Statement by Honorable Paul McHale, Assistant Secretary of Defense for Homeland Defense, Before the 109<sup>th</sup> Congress, Subcommittee on Terrorism, Unconventional Threats and Capabilities, Committee on Armed Services, United States House of Representatives, March 15, 2005.

Secondary Sources:

"All Homeland Security is Local." *Slate*. <http://www.slate.msn.com>. December 3, 2004 (accessed February 19, 2005).

Container Security Initiative, U.S. Customs and Border Protection.  
[http://www.cbp.gov/xp/cgov/border\\_security/international\\_activities/csi](http://www.cbp.gov/xp/cgov/border_security/international_activities/csi) (accessed September 25, 2005).

*Department of Defense Dictionary of Military and Associated Terms, Joint Pub 1-02.*  
Washington D.C.: U.S. Government Printing Office, 12 April 2001.

*Executive Order (EO) 12333*, [www.fas.org](http://www.fas.org) (accessed October 1, 2005).

“Integrated Undersea Surveillance System.” *Federation of American Scientists (FAS)*.  
<http://www.fas.org/irp/program/collect/iuss.htm> (accessed March 19, 2005).

*Joint Interagency Task Force South*. [www.jiatf.southcom.mil](http://www.jiatf.southcom.mil) (accessed January 8, 2005).

“Navy Chief Calls for Maritime Norad.” *The Patuxent Partnership*.  
<http://www.paxrivier.org>. May 2, 2005 (accessed June 4, 2005).

*Office of Naval Intelligence*. <http://www.fas.org/irp/agency/oni/intro.htm> (accessed September 30, 2005).

*The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks on the United States*. New York: W. W. Norton, 2004.

*Weapons of Mass Destruction*. <http://www.globalsecurity.org/wmd> (accessed March 5, 2005).

Ackerman, Robert. “Pace of Change Accelerates for U.S. Navy.” *Signal*.  
<http://www.afcea/signal.org>. Dec 2004 (accessed March 12, 2005).

Bhattacherjee, Anjali and Dolnik, Adam. “Hamas: Suicide Bombings, Rockets, or WMD?” *Terrorism and Political Violence*, Autumn 2002.

Bowyer Bell, Bower. *The Gun in Politics: An Analysis of the Irish Political Conflict*. New Brunswick: Transaction Publishers, 2003.

Capelotti, P. J. “The Coast Guard’s Response to 9/11.” *Joint Center for Operational Analysis and Lessons Learned*, Vol VI, Issue 4, September 2004.

Elsea, Jennifer. “The Posse Comitatus Act and Related Matters: A Sketch.” *CRS Report for Congress*. Washington D.C.: Congressional Research Service, June 6, 2004.

Flynn, Stephen. *America the Vulnerable*. New York: Harper Collins, 2004.

Fritz, Alarik. *Navy Role in Homeland Defense Against Asymmetric Threats*. Washington D.C: Center for Naval Analysis, 2001.

Gannon, Michael. *Operation Drumbeat*. New York: Harper and Row, 1990.

Grey, Colin. *The Leverage of Sea Power*. New York: The Free Press, 1992.

Groves, Eric. *The Future of Sea Power*. Annapolis: Naval Institute Press, 1990.

Hecker, J.Z. "Port Security: Nation Faces Formidable Challenges in Making New Initiative Successful." *GAO Publication No. GAO-993T*. Washington D.C.: United States General Accounting Office, 2002.

Johnson, K. and Wirtz, J. *Strategic Intelligence*. Los Angeles: Roxbury Publishing, 2004.

Lowe, Merrie Schilser. "Lack of Maritime Security Leaves U.S. Ports Open to Attack." NORAD press release, [www.norad.mil](http://www.norad.mil). September 8, 2004 (accessed March 12, 2005).

Miles, Donna. "Planning Group Weighs Value of 'Maritime NORAD.'" Armed Forces Info Service, *DefenseLink News*, May 17, 2005.

Preisser, Alan. "Understanding Authorities in National Security Events." *Joint Center For Lessons Learned Quarterly Bulletin*, Vol 5 Issue 1, Sept/Dec 2002.

Runyan, T. (ed). *To Die Gallantly: The Battle of the Atlantic*. New York: Westview Press, 1992.

Sample, Doug. "Coast Guard Faces Increasing Security Challenges." Armed Forces Info Service, *DefenseLink News*, May 17, 2005.

Spinetta, Lawrence. "Expanding NORAD: A Strategy to Engage Mexico." Air Power International, 24 June 2004. [www.airpower.maxwell.af.mil](http://www.airpower.maxwell.af.mil) (accessed April 30, 2005).

Sherman, Jason. "Domain Defense." *Sea Power Magazine*. [http://www.navyleague.org/sea\\_power](http://www.navyleague.org/sea_power). May 2005 (accessed February 26, 2005).

Strohm, Chris. "Military Bolsters Maritime Security Role." Daily Briefing at [www.govexec.com](http://www.govexec.com), March 26, 2004 (accessed February 26, 2005).

Swartz, Peter. *The Homeland Defense Role of the Navy*. Washington D.C: Center for Naval Analysis, 1998.

Tiron, Roxana. "Northern Command not Directing Enough Attention to Maritime Defense." *National Defense*, January 2005.

Treverton, Gregory. "Intelligence: Welcome to the U.S. Government." Johnson, L. and Wirtz, J. (ed) *Strategic Intelligence*. Los Angeles: Roxbury Publishing, 2004.

Trilbecock, C. "The Myth of Posse Comitatus." *Journal of Homeland Security*, October 2000.

Thomas, Guy. "A Maritime Traffic-Tracking System: Cornerstone of Maritime Homeland Defense." Newport: Naval War College Review, Vol LVI No.4, Autumn 2003.

\_\_\_\_\_. "A System Engineering Approach to Building an MDA System—Backbone to a Maritime Norad."

Watts, R.B. "Defending Our Shores." Annapolis: U.S. Naval Institute *Proceedings*, October 1987.

\_\_\_\_\_. "Coastal Defense: Now More Than Ever." Annapolis: U.S. Naval Institute *Proceedings*, December 1990.

\_\_\_\_\_. "Don't Forget Military Operations." Annapolis: U.S. Naval Institute *Proceedings*, April 1995.

## **INITIAL DISTRIBUTION LIST**

1. Defense Technical Information Center  
Ft. Belvoir, Virginia
2. Dudley Knox Library  
Naval Postgraduate School  
Monterey, California
3. Commandant (CG-7M)  
Coast Guard Headquarters  
Washington, D.C.
4. Captain Jeffrey Kline  
Naval Postgraduate School  
Monterey, California
5. Commandant (G-OPD)  
Coast Guard Headquarters  
Washington, D.C.
6. RDML Charles Martoglio  
Office of the Chief of Naval Operations (N5SP)  
Navy Pentagon  
Washington, D. C.